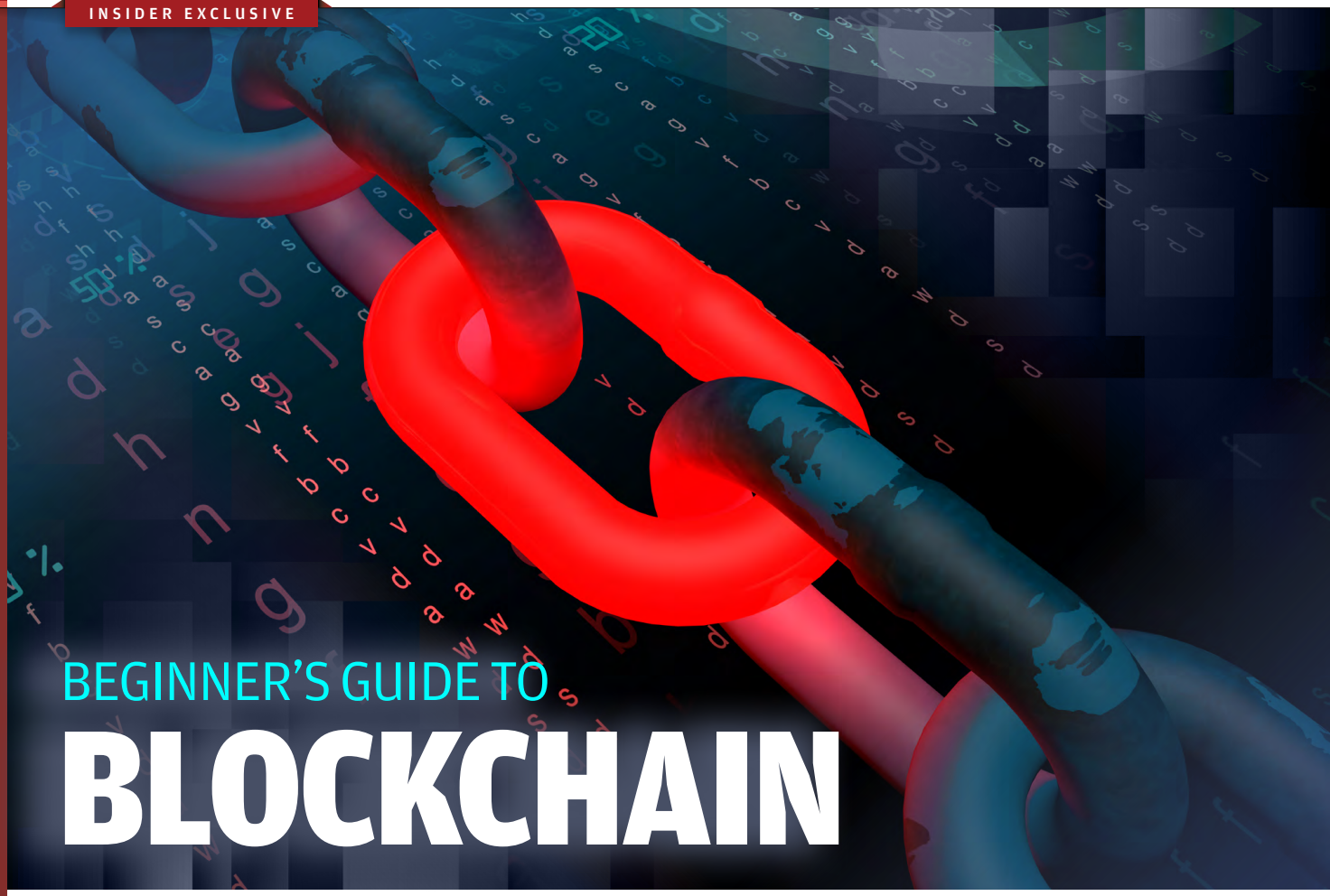
COMPUTERWORLD
FROM IDG

THE VOICE OF BUSINESS TECHNOLOGY

INSIDER EXCLUSIVE



BEGINNER'S GUIDE TO BLOCKCHAIN

Blockchain, the distributed ledger technology that began as the underpinnings of bitcoin, could revolutionize a variety of industries–everything from financial services to supply chains to personal identity and privacy online.

Here's what you need to understand the much-hyped technology and how it might be just the thing for business.

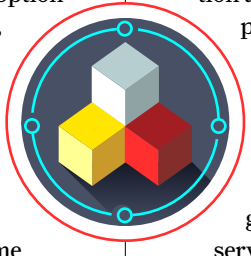
AKINBOSTANC / GETTY IMAGES

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**

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 distributed ledger technology (DLT), using a peer-to-peer (P2P) topology, blockchain allows data to be stored globally on thousands of servers—while letting anyone on the network see everyone else's entries in 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.

To comment on this story, visit Computerworld's Facebook page.

Recent hype around this relatively new technology is real because, in essense, it represents a new paradigm for how information is shared; tech vendors and enterprises, not surprisingly have rushed to learn how they can use 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 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."

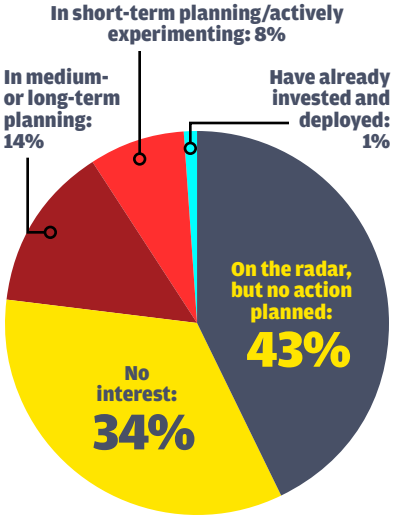
Martha Bennett, a principal analyst for Forrester Research, noted any blockchain or "DLT" project is a long-term strategic initiative, and disappointment is inevitable "when the hoped-for miracles fail to materialize.

"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."

BLOCKCHAIN PLANS

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.

What are your organization's plans in terms of blockchain?



Base: Total responses to Gartner in 2018, excluding those of 'don't know' [3,138].

SOURCE: GARTNER, INC.

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).

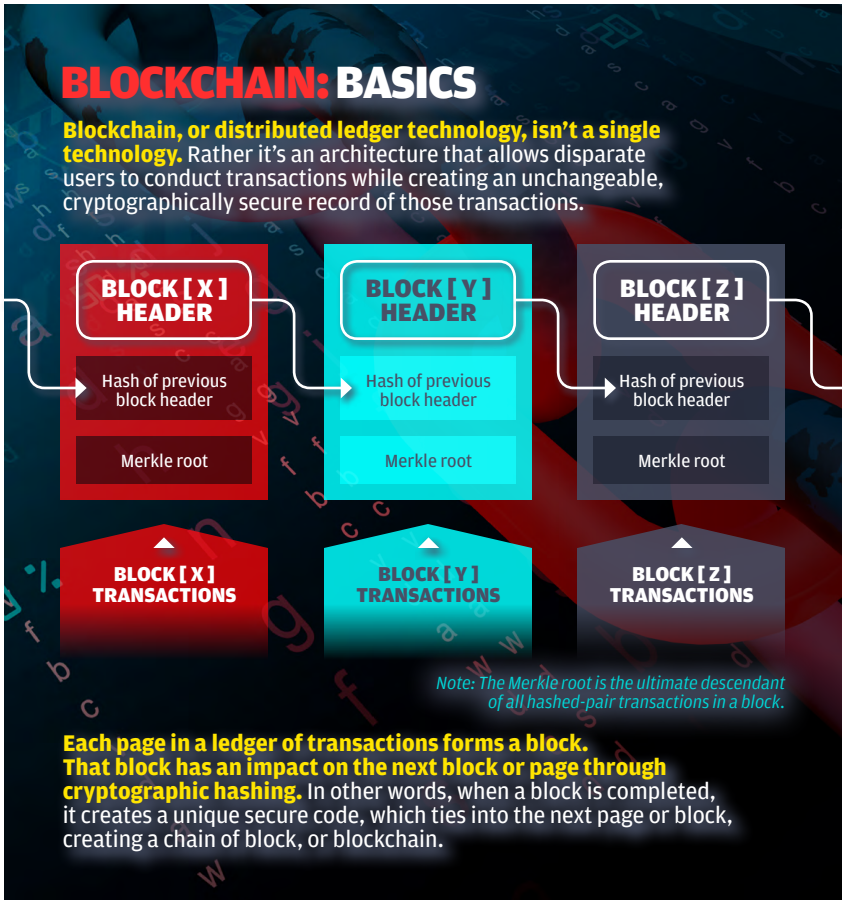
Blockchain can only be updated by consensus between participants in the system, and once new data is entered it can never be erased. It is a write-once, append-many technology, making it a verifiable and auditable record of each and every transaction.

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.

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 is beginning to change for cryptocurrencies. Earlier this year, J.P. Morgan Chase launched JPM Coin, its own cryptocurrency backed by fiat money that will enable one banking client to send money to another removing traditional settlement processes. In April, Visa and cryptocurrency exchange Coinbase created a debit card that will allow users to make purchases tied directly to their crypto wallets. And, in June, Facebook announced plans to launch a blockchain-based financial network and cryptocurrency in 2020 that will allow users to make purchases or transfer funds with just a couple taps on an app.

Governments have also 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.

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

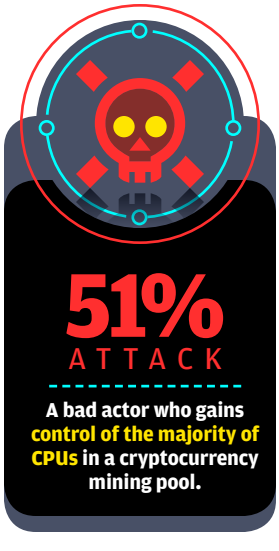
AKINBOSTANC / GETTY IMAGES

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.

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 launched 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.

> 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.
>
> **ALEX TAPSCOTT,** CEO + FOUNDER, NORTHWEST PASSAGE VENTURES



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.

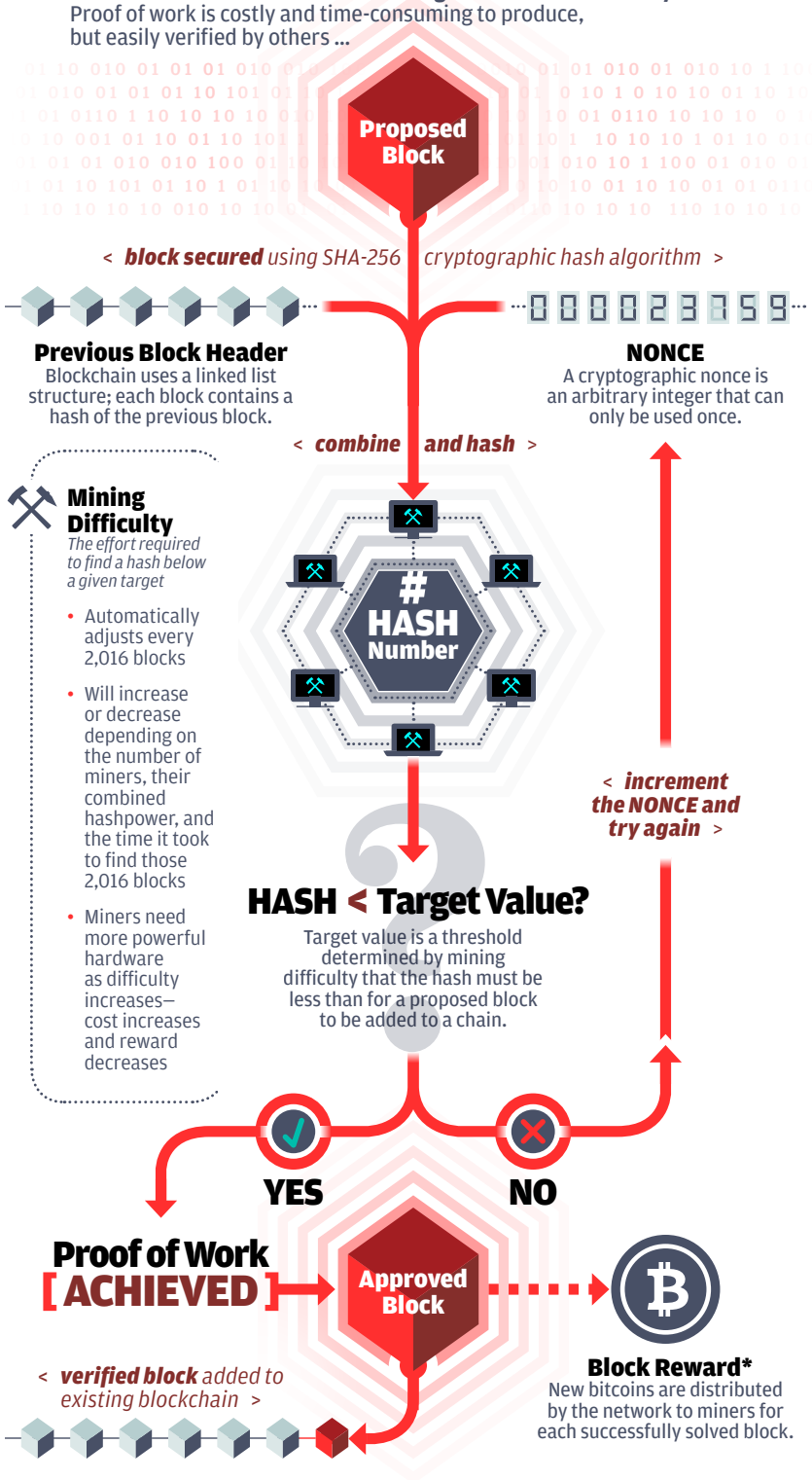
The computing resources needed for most blockchains are tremendous, Tapscott said, because of the number of computers involved. For example, the bitcoin blockchain harnesses anywhere between 10 and 100 times as much computing power as all of Google's serving farms put together.

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

BITCOIN: PROOF OF WORK

Proof of work is a Blockchain protocol for verifying transactions on a decentralized network and maintaining consensus across the system. Proof of work is costly and time-consuming to produce, but easily verified by others ...



fewer nodes because they're more susceptible to a single person seizing control based on a Proof of Work (PoW) consensus mechanism.

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 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

* *Block rewards are the only way new bitcoins are created on the network.*

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 second.

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.

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.

90% **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.

MAERSK

"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.

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.

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.

> Blockchain capabilities have allowed us to **rethink how critical information can be sourced and exchanged** between global banks.
>
> **EMMA LOFTUS,** HEAD OF GLOBAL PAYMENTS AND FX AT J.P. MORGAN TREASURY SERVICES

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

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

"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

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

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.

To comment on this story, visit Computerworld's Facebook page.

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

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.

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.

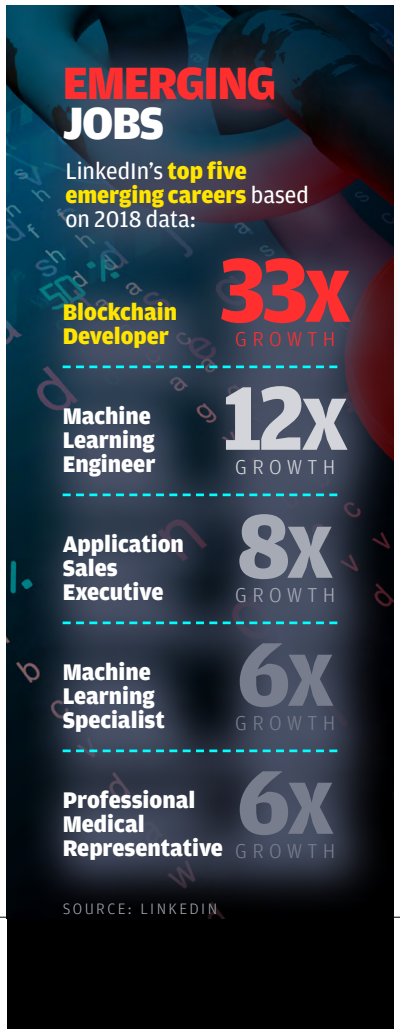
Blockchain careers are taking flight

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.

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.

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.

AKINBOSTANC / GETTY IMAGES

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.

"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.

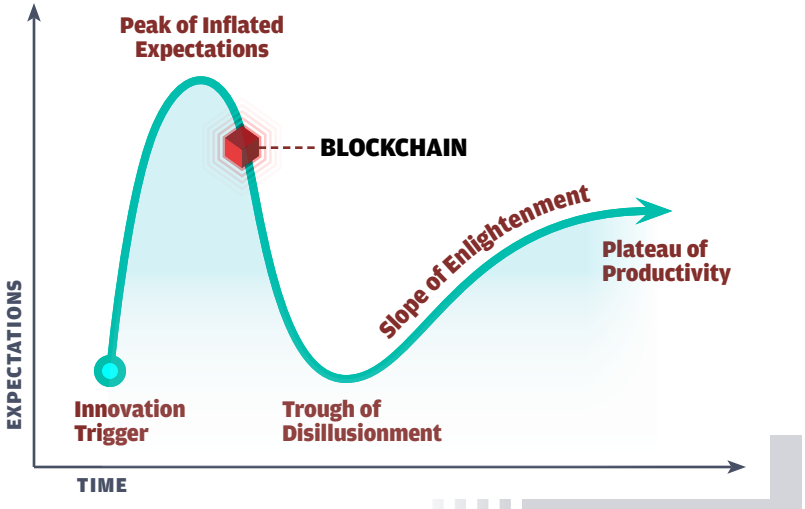
"When we started this in the 1970s, no one anticipated I could be in Boston and FaceTime with my mobile device with someone in Shanghai. That was science fiction," Harvard's Lakhani said.

"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." ◆

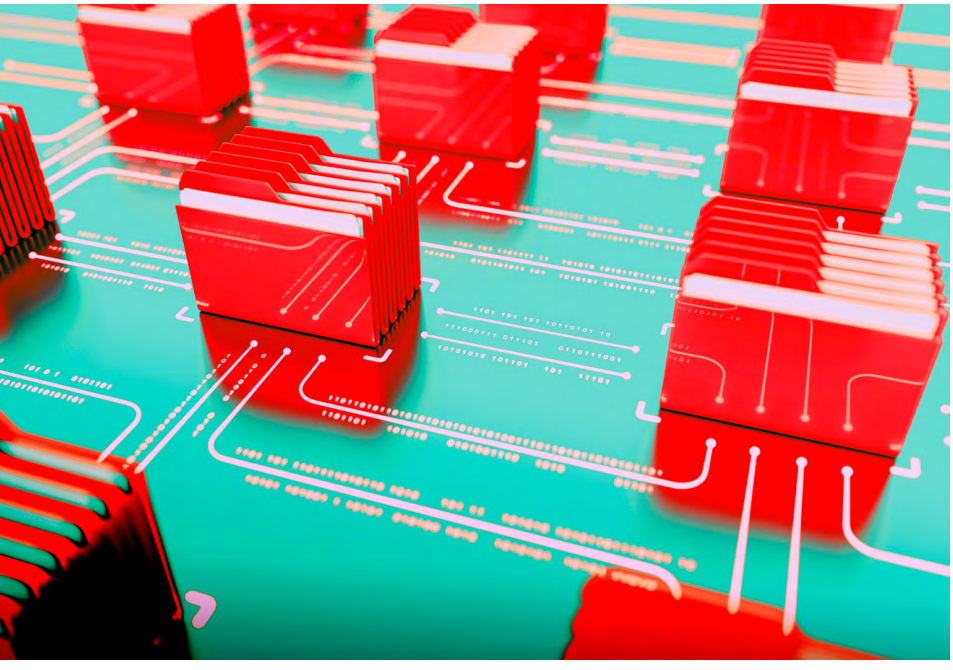
Senior Reporter **LUCAS MEARIAN** *covers financial services IT (including blockchain), healthcare IT and enterprise mobile issues (including mobility management, security, hardware and apps).*

BLOCKCHAIN HYPE

Garner's Hype Cycle for new technolgies | 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.



SOURCE: GARTNER, INC.

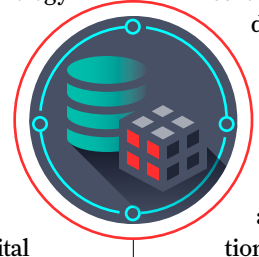


BLOCKCHAIN VS. DATABASE

WHAT'S THE DIFFERENCE?

Although blockchain has been accused by detractors of being nothing more than a more complicated and expensive database, **blockchain has one unique feature that a database will never replicate.** BY LUCAS MEARIAN

BLOCKCHAIN distributed ledger technology (DLT) has been touted as the answer for just about every transactional issue facing the world today—from payment processing and supply chain tracking to digital identities and copyright protection.



Databases, however, have been serving those same use cases for decades. They record how much money is in a bank account, when cargo reaches a destination and they store the identities of business users—enabling access to business applications and sensitive data. Because of those similarities, there are cynics (some may even call them pragmatists) who believe once you strip away the hype associated with blockchain and its cryptocurrency origins, what you have left is nothing more than a fancy, but slow and expensive, database.

The argument goes that many of the purported attributes of blockchain can be accomplished with conventional, tried-and-true technology. For instance, there are already hashing algorithms, digital signatures and public key infrastructure (PKI) available for use. If you need a traceable, verified audit trail, you can save your transactions to a database and then digitally sign the data, hash it and store that hash.

To comment on this story, visit Computerworld's Facebook page.

The difference: blockchain has all of those features in one place and it plays well with others.

"There is value in blockchain in and of itself as a distributed, independently verifiable single version of the truth shared amongst multiple entities—where no one entity is in control and all entities have equal access and equal control," said Avivah Litan, a Gartner vice president of research.

"It's also true that you can get non-blockchain technology to support basically the same thing—a distributed independently verifiable single version of the truth shared amongst multiple entities. But, those functions are not built into the technology as it is with blockchain DLT," Litan added.

D3DAMON / GETTY IMAGES

The difference between blockchain and a database

At a high level, both traditional databases and blockchain are data storage and data management infrastructures, explained Frank Xiong, Oracle's group vice president of blockchain product development.

Xiong agreed a traditional database can achieve what blockchain can "technically" by the party that owns and has access to the database. However, if multiple business parties need to perform transactions, they may not necessarily trust a single owner of the database, who creates, updates and keeps all the records.

helps to visualize databases as birds, with blockchain being a type of bird since it does have the same "DNA". (IBM is among a large number of software and services vendors, including Microsoft, Oracle, SAP and Amazon Web Services, who offer blockchain-as-a-service to their customers.)

Speaking at IBM's Think conference in San Francisco last month, Cuomo described DLT as akin to a database but with unique features not exhibited by other types of "birds," i.e., databases. For example, unlike databases, blockchains have shared ledgers, consensus algorithms, smart contracts and native data

> There is value in blockchain in and of itself as **a distributed, independently verifiable single version of the truth** shared amongst multiple entities–where no one entity is in control and all entities have equal access and equal control.
>
> **AVIVAH LITAN,** VICE PRESIDENT OF RESEARCH, GARTNER

"The biggest difference is the distributed ledger. We do have distributed databases, but most of them are owned by individual enterprises ... where they have databases distributed for different purposes," Xiong said.

"Blockchain ... technology is the preferred technology to create immutable transaction records and keep them in the distributed ledgers, of which every party on the chain has an identical copy and can [have] access to it," Xiong continued. "In the meantime, it accomplishes immutability, security, privacy and audit capabilities for every party on the chain"

IBM's vice president of blockchain technologies, Jerry Cuomo, said it

immutability—they are write-once, append many electronic ledgers.

Unlike a database administrator, who has access to commands such as "update" and "delete" that can change records in the ledger, once a transaction has been committed to a blockchain network, its community of administrators are powerless to change it. Each block (or record) is cryptographically secured to the previous block on the ledger, which creates a perfect audit trail.

"Unlike the database bird that has a single administrator who sets up the rules for the ledger, a blockchain ... has multiple administrators, each with an exact copy of the ledger," Cuomo said.

BLOCKCHAIN FORKS

A fork represents a change to protocol rules causing a blockchain to split into two potential paths forward ...

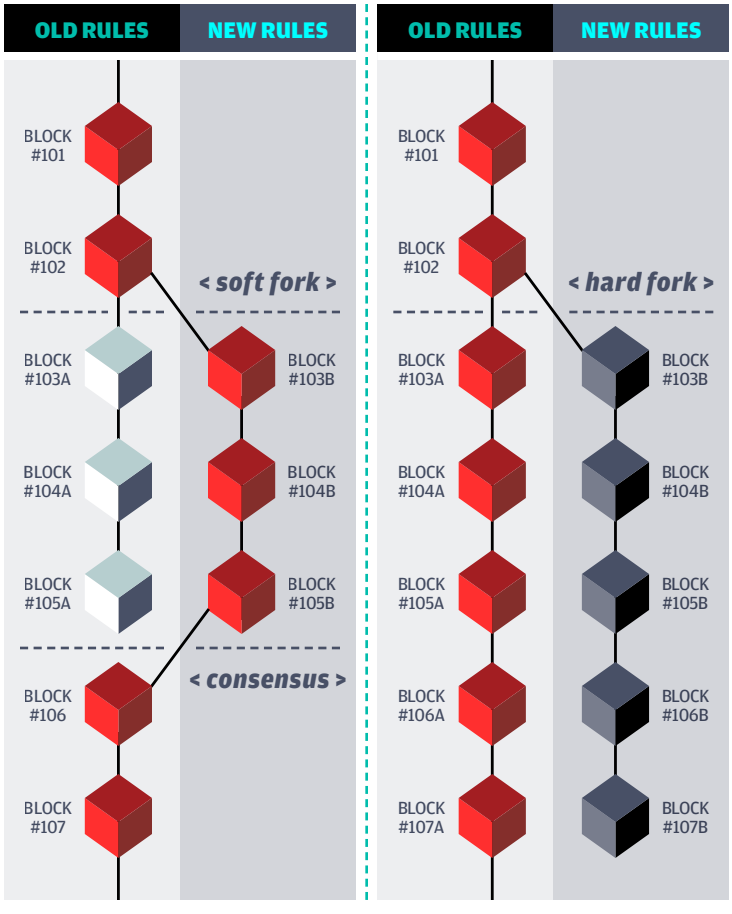
- Strongest chain of blocks
- Blocks in violation of new rules
- New forked chain

Soft Forks

Protocol changes that are **backward compatible** and which will be interoperable with the original blockchain's rules.

Hard Forks

Protocol changes that are not backward compatible and represent a **permanent divergence** in the blockchain.



In a database, the administrator controls what data is shared among users, and when a transaction gets submitted, it's immediately committed to that ledger.

Blockchain DLT is based on a peer-to-peer (P2P) decentralized architecture, with multiple administrators as part of its consensus protocol. In other words, transactions on a blockchain network are first proposed, then consented to by the group. Only if 51% of that group agree the transaction is acceptable is it then added to the ledger.

Blockchain's consensus protocol also means it is fault tolerant and it can continue to operate even in the presence of bad actors because a majority of users will keep transactions honest.

Permissioned vs. public blockchains

Not all blockchains are alike. For example, some blockchains are public—such as bitcoin—while others are private or permissioned, such as Hyperledger Fabric, R3 Corda and Ripple. In a public blockchain, anyone can sign up to become another node in the network and submit transactions to it. And, anyone can see those records (such as bitcoin transactions).

In a permissioned blockchain, the originator of the ledger determines who can join, see the transactions and submit new blocks. Yet, every authorized node in the chain still has say over what data is approved for the record. Network members are known and identified by membership PKI keys issued by a decentralized certificate authority.

Additionally, the promise of decentralized consensus on top of permissioned blockchain transactions could eventually enable parties anywhere who don't necessarily trust each

other to conduct business in a trusted fashion, according to Litan.

Unlike a database, theoretically, each entity that participates in a permissioned blockchain network can run a consensus/validation node; in practice, they don't, because they don't have the skills or the bandwidth for it. Instead, they typically relegate it to the project sponsor or vendor, Litan said.

"The common thinking out there is that once these companies get comfortable and gain expertise with blockchain, they will participate in transaction validation and consensus, along with the project sponsor or vendor," Litan said. "However, that isn't happening in the immediate future—not until public blockchain matures and scales."

Permissioned blockchains offer business automation tools through smart contracts. Smart contracts execute transparent, pre-determined rules and enable blockchain to avoid a central authority. Smart contracts operate on an "if this happens, then this executes" premise. For example, when a shipping company receives payment for a delivery, a smart contract in a supply chain blockchain can trigger the supplier to manufacture another product to fill the next order.

One myth is that once a smart contract has been written, a mistake can't be fixed or changes can't be made. In other words, you're stuck with the bad code.

Not so.

"In a permissioned environment, the ability to update smart contracts is a given, and it's designed into the frameworks," said Martha Bennett, a Forrester principal analyst. "You, of course, need a strong governance model, but then you also need that for public [blockchains]—technically, it doesn't take much to fork a chain."

BLOCKCHAIN SPENDING

Top five use cases based on 2019 market share
[*value / constant annual*]

1. **Cross-border payments, settlements** [15.9%]
2. **Trade finance, post trade/ transaction settlements** [10%]
3. **Lot lineage/ provenance** [9.8%]
4. **Asset/goods management** [8.6%]
5. **Regulatory compliance** [7.3%]

SOURCE: IDC WORLDWIDE SEMIANNUAL BLOCKCHAIN SPENDING GUIDE, 2018H1

Governance models allow blockchains to temporarily or permanently split or "fork," creating a new branch of blocks. A hard fork is a permanent divergence from a previous blockchain; a soft fork is a temporary change that is backward compatible. Think of a railroad train changing tracks through a switch; in a blockchain, the switch would be governed by the majority with power over the railroad service.

For example, the Linux Foundation's Hyperledger Fabric is a permissioned blockchain platform. That means all participants are, to an extent, identified and that the blockchain comes with a proper governance to resolve issues that may arise.

When to use a blockchain instead of a database

Forrester's Bennett said companies shouldn't really use a blockchain unless the use case really calls for that type of architecture, because distributed systems always add overhead, and many of the algorithms and techniques are still in their infancy.

There are two key questions for a company considering blockchain:

1. Does the ecosystem (or the initiator of the distributed ledger network) have a good reason for not wanting to share data via a single, centrally controlled system?
2. Does the company want to address use cases involving automated processes running across corporate boundaries and/or leverage the potential of tokenization? (Tokenization is the digital representation of a commodity, such as money or physical goods.)

Where blockchain technology shines is when multiple organizations are involved, according to Joel Weight, COO at Medici Ventures. (Medici Ventures, the venture capital arm of Overstock.com, has been investing heavily in blockchain technology, including dozens of start-ups. Five years ago, Overstock.

com began accepting bitcoin as a form of payment.)

"My bank doesn't need a blockchain to track the balance of my checking account, or to transfer funds from my checking account to my savings account," Weight said. "In that case, the bank is just moving money from one pocket to another, which a fast, secure database is perfectly suited for."

Where blockchain can be useful is when two organizations have a proprietary view of the world, each stored in their own databases. In order to share that data, there's a cost involved to ensure each company's view of the data is the same or to ensure both parties actually have the assets they expect to exchange, Weight explained.

For example, if instead of using escrow services or following an expensive, slow protocol, all parties work from the same data, then costs to normalize data and trust is minimized. Attepting to do that with a database would require one company to be the owner of all the data—and the source of "truth" for everyone involved in the transcation.

"The permissioned blockchain only requires enough trust between institutions to decide who will participate in the network, then the blockchain takes care of keeping participants honest once they join the network," Weight said. "The permissioned blockchain network would allow the atomic transfer of value between institutions where both can instantly agree on the state of the ledger before and after the transaction has occurred."

Though many companies still confuse the differences between blockchain and traditional databases, DLT seems set to grow quickly over the next few years as companies move beyond pilot programs.

Worldwide spending on blockchain solutions is forecast to be nearly $2.9 billion this year, an increase of 88.7% from the $1.5 billion spent in 2018, according to a newly updated Worldwide Semiannual Blockchain Spending Guide from IDC.

"Blockchain is maturing rapidly, and we have reached an inflection point where implementations are moving quickly beyond the pilot and proof of concept phase," said James Wester, research director for IDC's Worldwide Blockchain Strategies. ◆

> **The biggest difference is the distributed ledger.** We do have distributed databases, but most of them are owned by individual enterprises ... where they have databases distributed for different purposes.
>
> **FRANK XIONG,** ORACLE'S GROUP VICE PRESIDENT OF BLOCKCHAIN PRODUCT DEVELOPMENT

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

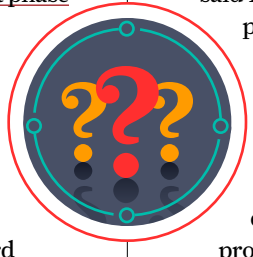
HOW TO DECIDE:

SHOULD YOU DEPLOY BLOCKCHAIN?

At a Forrester Research tech conference this week, principal analysts and the IT director for the Federal Reserve Bank of Boston talked about **how to deploy blockchain and who should consider doing so**. BY LUCAS MEARIAN

WHILE BLOCKCHAIN may have moved beyond the proof-of-concept phase and into limited production systems, that doesn't mean companies watching from the sidelines should plow ahead with their own deployments.

But neither can they afford to sit idly by.



"You can't catch up on innovation. If you wait until things have settled down, it may be too late," said Forrester Research principal analyst Martha Bennett.

Speaking at Forrester's New Tech & Innovation Conference, Bennett said public and private organizations must first determine what business processes blockchain distributed ledger technology (DLT) can address—and those to which it cannot be applied.

"Nothing is being revolutionized today from an enterprise perspective," Bennett said. "Quite frankly, it is a wild west out there. When you make comparisons with the early internet, which a lot of people do, there are indeed some parallels in that we really don't know where this is going to go yet. But that doesn't mean we shouldn't engage with it today."

Sorting out use cases

To determine if there is a use case, enterprises must first understand that while many existing technologies, such as relational databases, can already address most transactional business needs, they cannot match blockchain's key attribute: collaboration.

"Distributed ledgers are a team sport. It's about data you can trust to the highest degree possible and it's about sharing," she said.

Businesses should ask themselves whether multiple business units or other industry participants have the same issue or a related issue, such as transaction reconciliation problems, and what opportunity they can capture through blockchain.

For example, we.trade, a consortium of nine competing European banks, deployed a distributed ledger over which trade finance can be transacted for small- to medium-sized businesses. The DLT enabled the banks to continue

MATEJMO / GETTY IMAGES

to compete and it addressed a common issue: simplifying domestic and cross-border finance.

Bennett offered up a "check list" enterprises should consider when determining whether to deploy blockchain, including:

- When multiple parties need the same data and the ability to write to the same data store;
- When all parties need an assurance that data is valid, and hasn't been tampered with;
- When a current system is error-prone, too complex, too unreliable or full of friction points;
- When there are good reasons not to have a single centralized system, such as a relational database.

The Fed takes a look

Paul Brassill, vice president of IT for the Federal Reserve Bank of Boston, said his organization, while typically cautious, has been struck by the "hockey stick" effect of technology adoption over the past two decades, especially blockchain. The Fed first began exploring the use of Ethereum blockchain technology in 2016, then moved onto Hyperledger Fabric; it has invested significant resources determining how blockchain may affect, not only the national banking industry, but worldwide financial services.

"If the private sector can do it better than the Fed, then we need to do it better," Brassill said. "We started by uploading Ubuntu Linux and installed very simple smart contracts. Our learning along the way included the fact that our developers didn't know anything about this technology. We had to teach ourselves a lot of this."

The Fed's developers watched Youtube videos on how to use blockchain; one that was particularly useful, Brassill said, is an IBM-produced video about developing a blockchain with Hyperledger Composer.

The Fed's developers used Amazon Web Services to spin up a Linux virtual machine and download Ethereum Fabric.

A "pivotal moment" came when the Fed sent IT staff to Europe to talk to their counterparts at the Bank of England, which was exploring moving the nation's interbank settlement network onto Hyperledger because it is a "permissioned" blockchain, not an open DLT on which cryptocurrencies such as bitcoin are based.

"We realized a banking network of the future needs to have membership services; it needs to have more [encrypted] transactions, so we abandoned our Ethereum approach and started going in the Hyperledger approach," Brassill said.

The Fed's three blockchain pilots

The Federal Reserve Bank of Boston built three blockchain proof-of-concepts, first to test it as a general electronic ledger for the more than $6 billion it manages in reserve for the region's banks.

A second proof of concept tested what an audit or supervisory node in a distributed ledger might look like if it were part of a massive, digital national banking network.

"Would it do auditing or look for anti-money laundering challenges, or would it look for unusual fraud behavior and how would you digitize what is today a very human activity," he said.

"We have to build a spider web of connectivity between all of these banks where we're watching transactions over some massive blockchain environment and we're going to be in the middle of it," Brassill continued. "We're going to be ordering those transactions; we may be arbiter of the membership services deciding who gets to

> **This is a massive challenge, but I think it's one that's necessary** to see FinTech and DLT really impacting the financial market.
>
> **PAUL BRASSILL,** VICE PRESIDENT OF IT, FEDERAL RESERVE BANK OF BOSTON

be involved in this network, who issues certificates for it. This is a massive challenge, but I think it's one that's necessary to see FinTech and DLT really impacting the financial market."

A third blockchain PoC the Fed is building will run a non-critical HR application—one of its HR employee appreciation functions—but it will be run 24/7 to determine what problems might arise from constant use, such as scaling issues.

"Will we have storage issues ... smart contract development [challenges], what are the cyber risks?" Brassill said. "So, before we build out this mission-critical general ledger platform in the future, we first should get our arms around something very modest."

The Fed is aiming to roll out a production version of that blockchain-based HR app over the next year or so.

The agency is also examining how DLT could disrupt processes around the nation and the world, such as through micropayments—small online payments most often between consumers and retailers. And the Fed is looking at how blockchain could eventually affect large retail and wholesale payment platforms, such as the Automated Clearing House electronic network and Fedwire, which is used for large wholesale payments between banks.

"What if those platforms are running on distributed ledger technology? What are the cyber risks? How fast do they run? We need to understand that before we're disturbed," Brassill said. "Then there's this whole idea of fiat cryptocurrencies. ... The Fed needs to understand where this is going. What do ICOs mean for the economy? What do all of these 2,500 cryptocurrencies mean? By extension, what does this mean for the global eco-structure?"

The Federal Reserve Bank of Boston also has 300 examiners whose job it is to ensure the region's banks are liquid and stable.

"Picture a decade from now if some of those banks are running their credit system on blockchain; what might our examiners need to understand to better evaluate those companies?" Brassill said.

Using blockchain for larger networks

The Fed has been trying to determine where it stands in comparison to the world's other central banks in deploying blockchain because in the future there may be a global blockchain network through which banks transfer both traditional fiat and cryptocurrencies. It released a white paper earlier this year detailing its experiences rolling out blockchain PoCs—not only from a governmental but a business point of view, Brassill said.

The Boston Fed plans to tie into its PoC other Federal Reserve banks with the goal of creating a sandbox to test applications.

Because enterprise or "permissioned" blockchain's are distributed, anyone allowed into the electronic ledger by a central authority can potentially see every immutable data entry; that's extremely useful for business processes such as supply chain tracking or cross-border payment and settlement. Smart contract technology can also control who on a ledger gets to see what.

But, Bennett cautioned, smart contract technology belies its name: it is neither smart nor a legal contract. Smart contracts are business automation constructs (software coded to enforce predetermined rules) with the ability to achieve disintermediation of what are often manual processes.

And even when a business has successfully tested blockchain networks, even multiple times, it still doesn't mean the technology is ready for production because it still may not scale; it will need to integrate with existing business systems; and it will need to meet regulatory and compliance requirements that in many industries have yet to be determined.

"That's one of the reasons we're not going to see large-scale adoption immediately," she said. "Anybody who talks about DLT revolutionizing this industry, this process, this whatever—nothing is being revolutionized today from an enterprise perspective. What companies are doing is really looking at what they need to do today in order to do things differently in the future."

For example, in 2017, Northern Trust Corp. launched a commercial blockchain network based on Hyperledger Fabric for managing the administration of a private equity fund. The DLT network enabled real-time document exchange between all involved parties, and smart contract technology streamlined the approval process. Last month, The Chicago-based asset management firm handed its blockchain network over to private equity (PE) management solution to Broadridge for further improvement.

"They reduced the time taken to get together all the paperwork required for a private equity transaction from three weeks to three days," Bennett said, adding Northern Trust also allowed an auditor onto the blockchain in order to inspect the transactions in near real time, as opposed to the more traditional approach of performing periodic audits of long-completed transactions.

Why companies might avoid blockchain

Companies considering deploying blockchain should ask themselves whether there are good reasons not to have a single centralized system, because DLT introduces complexity and, at least today, still introduces risk because of a lack of maturity.

"Ultimately, only you know your organization and your industry well enough to be able to say this is where the shoe hurts and this is the process that's broken. What problem are you trying to solve with this?" Bennett said.

She cautioned that while there are parallels between the internet's early days and blockchain technology, in that both had the potential to become a ubiquitous communication vehicle, the glaring difference is blockchain has not undergone rigorous academic research.

"Typically, what you get, whether its artificial intelligence, or augmented reality, nanotechnology, or quantum computing is they tend to start in the research labs ... then they go into a commercialization phase for use in the real world, and then they go mainstream," Bennett said. "We've got networks running that are inviting commercial participation which haven't been undergoing any form of rigorous academic research."

What many of the public and private organizations that have deployed blockchain have learned that distributed ledger technology is far from fully baked and still faces hurdles that could take years, if not a decade, to work out.

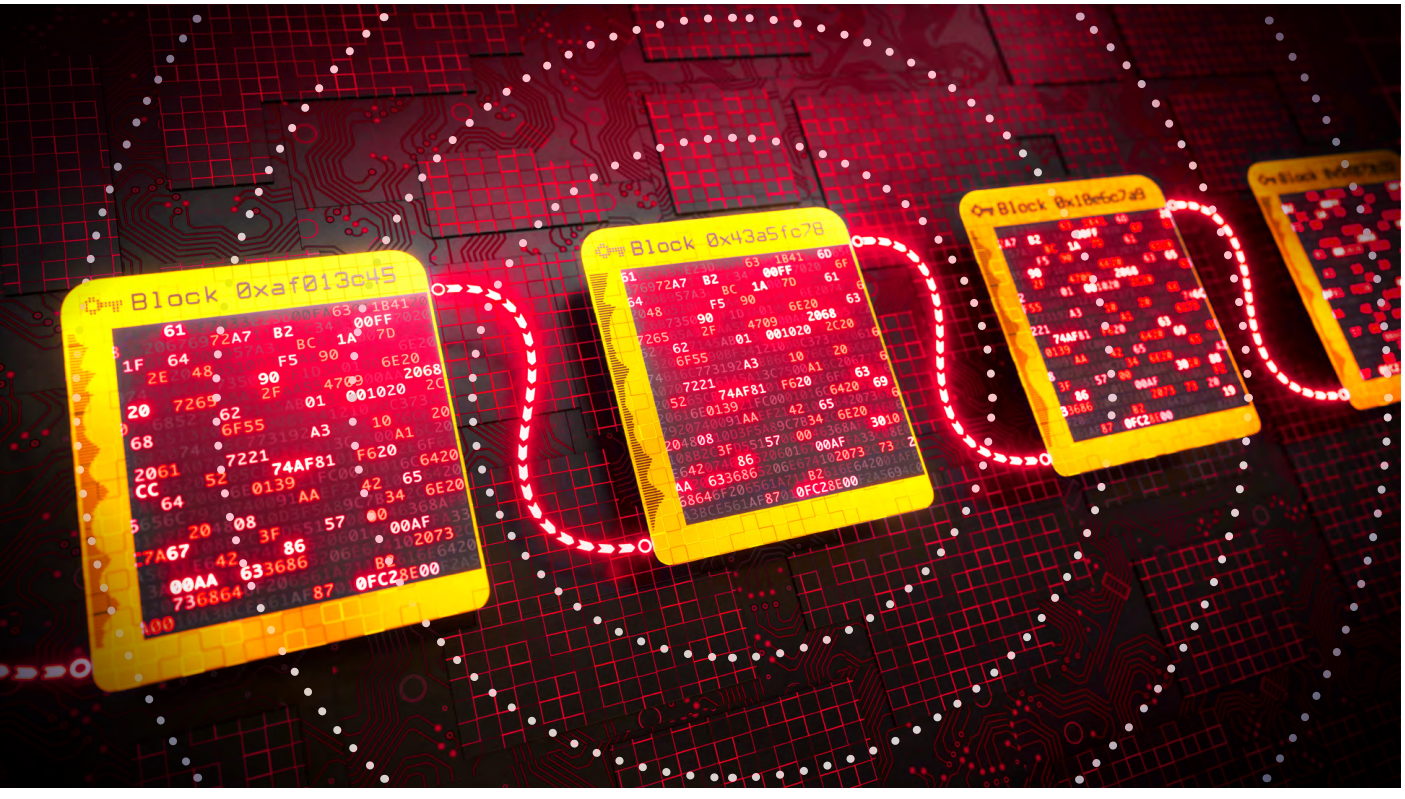
For example, there are still a myriad of competing specifications and blockchain iterations, so it's not known whether blockchain acceptance will be driven by standards, industry initiatives or de facto adoption.

"We'll have to wait and see," Bennett said. ◆

Ultimately, only you know your organization and your industry well enough to be able to say this is where the shoe hurts and this is the process that's broken.

MARTHA BENNETT, PRINCIPAL ANALYST, FORRESTER RESEARCH

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

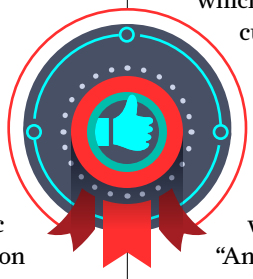


BLOCKCHAIN SUCCESS

MAKING BELIEVERS OUT OF ONE-TIME SKEPTICS

Walmart and IBM are among the companies that have embraced the distributed ledger technology, with the big-league retailer making it a key part of its supply chain future. **BY LUCAS MEARIAN**

FRANK YIANNAS, Walmart's vice president in charge of food safety, was once a "major skeptic" and "non-believer" in blockchain, the electronic ledger technology platform on which bitcoin and other cryptocurrencies are built.



"I always advise people: if you're a skeptic, stay in it; read, learn and more than that, try to do some work in it," Yiannas said. "And, I've come around and I've become a believer. For me ... it's more like a religious conversion. The more I got into blockchain, the more I thought this is the solution."

The problem Yiannas wanted to solve? How to track the origin of every piece of fruit, meat or vegetable sold by a worldwide retailer of food with 12,000 stores—and tens of thousands of suppliers.

"There are these big, mighty food companies, but they have a weakness," Yiannas told attendees at the "Business of

MATEJMO / GETTY IMAGES

Blockchain" conference at MIT last year. "I think the food system has one major Achilles' heel. Their Achilles' heel is a lack of transparency."

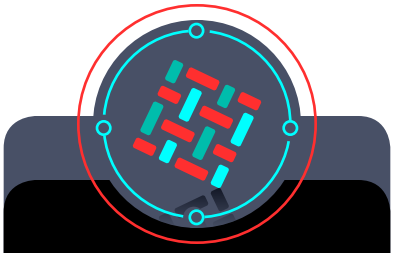
In 2017, Walmart and nine other food retailer giants including Dole, Driscol, Tyson, Nestle and Unilever teamed up with IBM to pilot a cloud-based blockchain technology as a unifying electronic ledger. The ledger, called Food Trust, was built using Hyperledger Fabric, an open-source blockchain platform run under the Linux Foundation's Hyperledger group.

When the food chain meets blockchain

Walmart tested the blockchain by tracking the origin of its mangos and pork; Yiannas said it worked flawlessly, solving a lack of transparency that permeates not only Walmart, but the world's food supply chain.

The lack of transparency was highlighted last year when grocers around the U.S. began pulling packages of romaine lettuce from their shelves after 53 people in 16 states became infected with E. coli linked to the vegetable.

The contaminated lettuce was determined to be from the Yuma, Arizona region, but the Centers for Disease Control and Prevention (CDC) said no single supplier had been identified—and unless retailers and consumers can confirm where the lettuce came from, all romaine should be thrown away. The CDC has warned consumers that most package labels do not identify growing regions.



The Linux Foundation's
HYPERLEDGER FABRIC

A permissioned blockchain platform. All participants are, to an extent, identified and the blockchain comes with proper governance to resolve issues that may arise.

The food supply chain today is not a "chain" at all, Yiannas argued, but is instead a fragmented, paper-based system; even when part of the supply chain is digitized, the various systems are unable to communicate with each other.

"For regulatory purposes, we're only required to have one step up and one step back traceability. Why do you think health officials are saying, just throw away all your romaine?" Yiannas said. "If you look at the FDA website, it says this today: It takes us hundreds, sometimes thousands of documents to piece together where the product came from.

"The idea that in the 21st century, after the spinach outbreak in 2006, we're still not at the point where you can scan a package of spinach and find out where it comes from is just not acceptable," he said.

In December 2017, to test Walmart's produce traceability, Yiannas grabbed a package of sliced mangoes from a store across the street from Walmart's Fayetteville, Ark. headquarters. and brought it back to a conference room. He challenged his team to find out from where the fruit came, an effort that took six days, 18 hour, and 26 minutes to get an answer, Yiannas said.

"We do better than most," he said.

In an early pilot of the IBM-run blockchain supply chain, Yiannas again tried tracking mangoes that had been entered onto the distributed electronic ledger, and was able to find the origin in 2.2 seconds.

"Blockchain for us is solving the complexity of many-to-many relationships. The idea that a supplier can get in and then share that information with whomever they want to is really powerful, and suppliers are really interested in that," Yiannas said.

Apart from using antiquated technology, part of the problem for the food industry is the sheer number of products available today. In 1980, a typical grocery store carried about 15,000 SKUs (a stock keeping unit that refers to a specific product). Today, the average grocery offers 50,000 individual food items, Yiannas said.

In the near future, the world's food supply chain will be "omnichannel," where any consumer can purchase any kind of produce from anywhere in the world and have it shipped to their doorstep. "While things are getting better for consumers, things are getting more challenging for those who have to manage the risk," Yiannas said.

Public vs. private blockchains

Blockchain ledgers can solve the complexity and traceability of goods shipments by enabling everyone on the network to see each

To comment on this story, visit Computerworld's Facebook page.

transaction, from the time a vegetable is handed off by a grower to a shipping company to its arrival at a national and then regional warehouse, right down to the retailer who places it on a store shelf. Each handoff is scanned into the electronic ledger, which then uses a randomly-generated number or hash to verify that transaction. Each set of transactions involving a particular good becomes an unchangeable entry, or block, on that ledger and can be used for auditing purposes.

There are a variety of blockchain permutations, but they fall mainly into one of two categories—public and private (also known as "permissioned"). Public blockchains allow anyone to see or send transactions ,as long as they're part of the consensus process; bitcoin is an example of a public blockchain.

A permissioned or private blockchain, in contrast, is centrally managed and restricts ledger entries to pre-vetted entities; a permissioned blockchain could be within a single company with many global branches or a group of companies who've partnered for a specific business purpose. Who can see the information on a permissioned blockchain can also be protected by a private/public hash key system.

Though it's early in terms of the technology's use in enterprises, there are very promising signs of its efficacy.

How blockchain is breaking out

Bridget van Kralingen, senior vice president of IBM Global Industries, Platforms and Blockchain, said blockchain is already showing great promise for use in a myriad of industries.

> **We do believe this tokenization of almost any good or service will take hold and take root.** We're actually seeing it being put to good in many places that aren't just about big companies.
>
> **BRIDGET VAN KRALINGEN,** SENIOR VICE PRESIDENT OF IBM GLOBAL INDUSTRIES, PLATFORMS AND BLOCKCHAIN

"In the financial services industry, we're seeing some really quite radical use cases take hold and take scale," van Kralingen said. "We do believe this tokenization of almost any good or service will take hold and take root. We're actually seeing it being put to good in many places that aren't just about big companies."

Tokenization involves the conversion of the rights to goods and assets into a digital token that can be tracked on a blockchain. The assets could be stocks and bonds, real estate, oil, cars, or whatever asset you wanted to buy or sell on an electronic ledger.

For example, 40% of small- and medium-sized businesses in Europe are unable to attain financing to export goods; the process is simply too complicated and expensive.

In 2017, five banks partnered with IBM to create a permissioned blockchain called Batavia through which SMBs could receive financing for international trade. More than 26 businesses have joined the electronic ledger on which they share identification and credit information across geographical and banking boundaries. Cross-border trade finance issues that once took 45 days to resolve could be squared away in less than 10, van Kralingen said.

In October, 2018, Batavia merged into We.Trade and together with IBM and 12 of Europe's largest banks they are continuing to build and host a trade finance platform to simplify and facilitate domestic and cross-border trade for small and medium enterprises in Europe, while helping to increase transparency in trade. The banks include: CaixaBank, Deutsche

Bank, Erste Group, HSBC, KBC, Natixis, Nordea, Rabobank, Santander, Societe Generale, UBS and UniCredit

CaixaBank, Erste Group and UBS joined from the Batavia trade finance network. In addition, UniCredit AG and Eurobank have joined as licensees, meaning the network now operates in 14 European countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland and the UK. In October 2018 We.Trade announced a collaboration with eTradeConnect, a trade finance consortium of 14 Hong-Kong banks.

Blockchain, van Kralingen said, actually changes the way the business world stores and manages data. "And, it's not done by some powerful technology vendor; it's done by the members of the network. It actually has a single, shared version of the truth," she said.

"Trust is at the lowest level in the last 10 years for governments and institutions. [Blockchain] has the ability, I think, to give us a technology that can underpin a business model which is around trust, transparency and permissioning," van Kralingen added.

Blockchain—because of its self-policing security and immutability—eliminates huge amounts of record keeping, which can get confusing when multiple parties are involved in a transaction, said Saurabh Gupta, vice president of strategy at IT services company Genpact.

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, those systems are often separate and require multiple parties to sign off on cargo shipments, creating a lengthy administrative process.

"There are more than 200 elements of information exchange. It's this complex [series] of relationships that is really creating this mess," Gokcen said. "There's a lot of inconsistent information that's ... prohibiting the flow of goods. Peer-to-peer messaging between those parties is extremely costly, cumbersome, extremely labor intensive.

A NEW BLOCKCHAIN BASED, DISTRIBUTED ELECTRONIC LEDGER could save the shipping industry billions of dollars a year by replacing a current EDI and paper-based system for tracking cargo and attaining approval from customs and port authorities.

Ibrahim Gokcen, chief digital officer at A.P. Moller–Maersk, the world's largest container shipment operator, said there can be as many as 30 entities and 100 people involved in shipping one container of avocadoes from Kenya to a main shipping terminal in Rotterdam.

"There's a lack of information sharing; that they don't trust each other was a huge impediment to progress," he added.

To try to streamline that process, Maersk in March 2017 announced it was testing a block-

chain-based ledger to manage and track the paper trail of tens of millions of shipping containers by digitizing the supply chain. In January 2018, Maersk teamed up with IBM to roll out the proof-of-concept shipping platform.

The Denmark-based company has been piloting the blockchain platform with various customers, including DuPont, Dow Chemical, Tetra Pak, Port Houston, Rotterdam Port Community System Portbase, the Customs Administration of the Netherlands and U.S. Customs and Border Protection.

shipping information for all parties involved, from manufacturers and shippers to port authorities and government agencies.

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 creates an immutable record, no one party can modify, delete or even append any one of the blocks without the consensus of others on the network.

required approvals are in place, helping to speed up approvals and reduce mistakes.

Companies who want in on the blockchain ledger can use a set of APIs to join it to their existing shipping systems through any data visualization application, such as Tableau or Spotfire. "This is paperless trade, and paperless trade allows the end users to submit, authorize and exchange documents all on a blockchain platform," Gokcen said. "Documents themselves are stored off-chain in a secure database, but the events

> **This is paperless trade,** and paperless trade allows the end users to submit, authorize and exchange documents all on a blockchain platform.
>
> **IBRAHIM GOKCEN,** CHIEF DIGITAL OFFICER, A.P. MOLLER-MAERSK

Joining forces: IBM and Maersk

In 2018. IBM and Maersk launched New York-based TradeLens, their blockchain-based shipment tracking system. The blockchain-based supply chain network launched with initial 94 participants piloting the system, including more than 20 port and terminal operators.

Maersk will make the electronic tracking system available to not only its customers, but it will sell it to other shipping companies as well. "We at Maersk will have zero preferential treatment from that entity," Gokcen said.

The blockchain-based shipping network will enable a single view via a virtual dashboard of all goods and

"This open platform is similar to an apps store where ... it's possible for different participants to build their own applications," Gokcen said.

The platform began with core applications: A shipping information pipeline that provides real-time, end-to-end supply chain visibility to all authorized parties who can securely exchange information about shipment events; and the "Paperless Trade" app that will digitize and automate paperwork filings by enabling end-users to securely submit, validate and approve documents across organizational boundaries.

In a similar vein, blockchain-based smart contracts—a business automation tool—ensure that all

or transactions related to them are stored on the blockchain.

"This creates a one-to-many relationship to remove the barriers of global trade, to eliminate inefficiencies, to reduce transaction costs and to remove some of the middlemen who are not creating value," he added. "There are lots of middlemen ... who just buy low and sell high. Those are the middlemen we're trying to eliminate from our supply chain." ◆

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

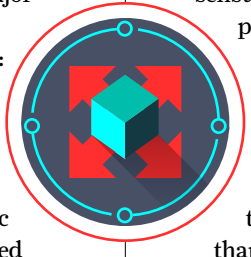
BLOCKCHAIN PHASE 2:

WILL IT SCALE?

As blockchain grows in popularity, so does the conundrum of **how to scale it while maintaining or boosting performance** so it can compete with today's transaction networks. **BY LUCAS MEARIAN**

MORE THAN ONE organization has been working on solving a major blockchain conundrum: how to improve sluggish transaction performance.

Blockchain distributed ledgers work by linking together a chain of electronic records, each inextricably tied to the one before it; each new set of entries or "blocks" is completed and time-stamped with a hashtag only after passing through a consensus process on a peer-to-peer (P2P) network.



Due to its chain nature, each new record inserted into a blockchain has to be serialized, which means—as the blockchain grows—the rate of updates is slower than traditional databases that can update data in parallel.

Today, the world's most popular cryptocurrency ledgers—bitcoin and Ethereum—use a proof of work (PoW) consensus model that requires nodes (servers) to complete a complicated mathematical problem as a way of authenticating new blocks (similar to how CAPTCHA acts as a challenge/response mechanism for websites confirming human users).

PoW mechanisms are slow by design. Bitcoin, for example, needs around 10 minutes to add a new record or block to the ledger, even with only 1MB of data allowed per entry. While there's no such limit on block size in Ethereum—it's been adjusted dynamically over time—it can only process about 20 transactions a second. By comparison, Visa's financial network processes about 10,000 transactions per second at peak load.

Complicating matters: neither bitcoin nor Ethereum P2P networks were designed to store large amounts of data; they simply do it by default. Because of that, as the electronic ledgers grow organically, so, too, does the compute and electrical power required to support them.

Various solutions have been proposed for addressing storage issues and speeding up the transaction process—from increasing block sizes to changing the consensus mechanism from PoW to proof of stake (PoS); the latter creates "bonded validators," or users, who must place a security

deposit down before they can serve as part of the blockchain consensus or voting community. As long as bonded validators act honestly on the blockchain, they remain in the consensus community; if they attempt to cheat the system, they lose their stake (their money).

Casting about for the right answer

In 2017, Ethereum introduced a PoS mechanism on a testnet called "Casper" (as in Casper the friendly ghost).

"Proof of Stake algorithms definitely have the potential to overtake Proof of Work," said Vipul Goyal, an associate professor in the Computer Science Department at Carnegie Mellon University (CMU). "However, there are still some significant research challenges that need to be overcome before that happens."

(There are also hybrid models that combine PoW with PoS mechanisms—giving deference to those with a vested interest while still allowing some degree of transaction validation from all users on the electronic ledger.)

Last year, the Ethereum Foundation reached out to outside developers to help solve its inability to sufficiently scale.

The foundation has explored two possible fixes. The first, known as layer 2, offloads the cumbersome back-and-forth processes between network participants to a separate blockchain or database. But it still allows the primary or layer 1 blockchain to record the final transaction result, i.e. you have purchased one Ether or bitcoin. Also known as "state channels," layer 2 would vastly increase efficiency by moving the most mundane processes off-chain while maintaining blockchain's innate trustworthiness.

> **Proof of Stake algorithms definitely have the potential to overtake Proof of Work.** However, there are still some significant research challenges that need to be overcome before that happens.
>
> **VIPUL GOYAL,** ASSOCIATE PROFESSOR, COMPUTER SCIENCE DEPARTMENT, CARNEGIE MELLON UNIVERSITY

Another possibility: 'Sharding'

The second potential fix involves moving to PoS and adding "sharding," which divides nodes on the network into partitions, each of which would be responsible for processing a small piece of each transaction, allowing many more transactions to be processed in parallel at the same time; sharding also isn't expected to diminish the native security of a blockchain because it maintains "most of the desired decentralization and security properties of a blockchain," Ethereum co-creator Vitalik Buterin wrote in a blog.

But, sharding is complex and it will take time to create a workable scheme, according to Ethereum's other co-founder, Joseph Lubin.

"We're not going to get to scalability instantly via proof of stake and sharding, so that's going to happen as phase three in our ecosystem," he said. "And I think that's going to be pretty profound. But the layer 2 solutions are a very powerful stepping stone."

Bitcoin and Ethereum developers have both proposed offloading transactional data to a secondary database or blockchain, which would allow funds to be transferred "off chain," keeping only the funds validation process on chain. Earlier this year, Bitcoin developers proposed the Lightning Network as a "second layer" payment protocol that could allow transactions and microtransactions to take place almost instantly on a separate P2P network.

While speaking at last year's Rise conference in Hong Kong, Lubin mentioned Plasma, a second-layer scaling fix for Ethereum, which would add tertiary blockchains for processing to a main, or layer 1, blockchain. Plasma was first introduced in

2017 by Buterin and Joseph Poon, who also created bitcoin's proposed Lightning Network.

"We're moving into a space where Ethereum can serve as the layer 1 trust system, and built into Ethereum we'll have hundreds of thousands of transactions in the layer 2 systems and we're going to see that ramified this year," Lubin said during a panel discussion.

In an interview with *Computerworld*, Lubin confirmed the trajectory for a layer 2 protocol in Ethereum: it could be constructed using Plasma for the purpose of gaming or a cryptocurrency exchange, which would then link back to a layer 1 Ethereum blockchain via a smart contract. (Smart contracts are business automation scripts that execute based on pre-determined rules).

The smart contract would be responsible for moving transactions between the root or layer 1 blockchain and the layer 2 blockchain; smart contracts would also maintain rules, such as not allowing a digital token, represented by a hash record, to be spent more than once. The layer 2 blockchain could also use other consensus mechanisms, such as PoS or even Proof of Authority, to validate transactions moving from a primary to a secondary blockchain.

"If something goes wrong on that system, the Plasma technology enables people to potentially pull their tokens out of that system based on the last checkpoint of recovered value, and there's nothing the managers of that layer 2 system can do to thwart people's ability to rescue their value," Lubin said.

And if you lose your cryptographic key?

Recovering cryptocurrencies when a system is hacked or a user loses their private cryptographic key has been an issue for as long as the distributed electronic ledgers have existed. If you lose your private key, you lose the ability to access your cryptocurrency.

One example of a layer 2 Ethereum blockchain could be an application enabling the purchase of Wi-Fi access at a coffee shop, say for a penny a minute. A customer would walk into the café and use the Ethereum-enabled application to sign in for Wi-Fi service. The application would allow the customer to set aside a certain amount of money in his or her account via an Ethereum smart contract. With each passing minute, the smart contract on the layer 2 blockchain would automatically record or validate another penny toward the Wi-Fi service charge. When the customer leaves, the final amount to be transferred would be recorded on the primary Ethereum blockchain. The café owner has the last transaction automatically signed by the smart contract when the service ends, which entitles him to the money owed.

Blockchain has also become a popular platform for gaming. For example, one of the earliest and most popular blockchain-based games is CryptoKitties, where players collect, breed and trade virtual cats. Each cat represents a non-fungible digital token. Trading card games, such as Spells of Genesis and Force of Will, are also based on blockchain.

Plasma networks would also allow users to move between two different blockchain-based games.

"Let's say there are two different games on two different Plasma-based networks. If I have a digitally-scarce sword that I'm using in one game, I might want to move it back to Ethereum, maybe to trade it to somebody or to move it to some other ... game," Lubin said.

The most prominent layer 2 Ethereum project to date is Loom Network, an SDK kit that went live earlier this year and enables the creation of highly-scalable games and user-facing DApps. The layer 2 technology uses a PoS consensus mechanism for authenticating new blocks.

Still time to experiment

At this point, there's no rush to bring a layer 2 protocol to Ethereum, Lubin claimed, saying there are there are other "pruning mechanisms" available using the current architecture that would enable more efficiency.

"So, we're not in real danger and the system can grow significantly for quite a while," he said. "I think we can squeeze two to three times the amount of performance out of it despite ... deficiencies."

For example, in the next iteration of Ethereum, the block size may increase by 50% or 70%, allowing more data to be stored on chain. "That's in play right now," Lubin said. ◆

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