



Blockchain: An insider's guide

Table of contents

- 03** [Six industries that are using blockchain to drive business value right now](#)
- 06** [18 new IT jobs created by Bitcoin and blockchain](#)
- 08** [Five companies using blockchain to drive their supply chain](#)
- 10** [How Microsoft is positioning itself as a leader in enterprise blockchain adoption](#)
- 12** [Is blockchain overhyped?](#)
- 14** [How blockchain could save lives by getting medicine where it's needed](#)
- 16** [Universities are adding blockchain classes to help close the enterprise tech skills gap](#)
- 19** [Why using blockchain to track cobalt mining could lead to more ethical smartphones](#)
- 22** [Nine reasons to be cautious with blockchain](#)

SIX INDUSTRIES THAT ARE USING BLOCKCHAIN TO DRIVE BUSINESS VALUE RIGHT NOW

BY ALISON DENISCO RAYOME

[Blockchain](#) has proven to be the largest value of cryptocurrencies, with implications for almost every industry. And some companies are already using the emerging ledger technology in everyday business operations.

An October 2017 report from [CompTIA](#) found that 16% of companies had purchased blockchain-enabled tools, while 22% were developing tools using blockchain. Another 24% said they were exploring the technology, while the majority—38%—said they had no current plans to do so or were unsure of plans.

Early adopters are using blockchain for digital identity (51%), asset management and tracking (49%), regulatory compliance/auditing (49%), distributed storage (48%), smart contracts (45%), and cryptocurrency/payments (44%).

However, the technology remains mysterious for many companies. Here are six blockchain use cases that companies are leveraging right now.

PHARMACEUTICALS

New rules to ensure drug integrity from manufacturing to consumption could save up to a million lives each year. Life sciences and healthcare companies create unique serial numbers for units of medication and pieces of equipment, which are scanned, captured, and verified at their point of origin, according to Scott Allison, president of healthcare at logistics giant [DHL](#).

Applied the right way, blockchain can take track and trace serialization to the next level, cutting costs, elevating security and trust, eliminating error-prone data movements, and enabling real-time supply chain transparency. “Using blockchain, as each item moves through the supply chain, additional verified information is appended,” Allison said. “These blocks of data cannot be tampered with and are collectively validated by all stakeholders. The result is an end-to-end system that is simpler and more secure than anything we have seen before. It is more private, more transparent, and more efficient, with less risk, and it meets and exceeds global serialization requirements.”

DHL is working with Accenture to establish a blockchain-based track-and-trace serialization system in six areas worldwide. The system is now populated by more than 7 billion unique pharmaceutical serial numbers and handling more than 1,500 transactions per second, Allison said.

FASHION

[CGS](#), an organization providing business applications, enterprise learning systems, and outsourcing services, is hearing from fashion, apparel, and consumer goods clients that they are looking at new ways to streamline the supply chain through blockchain.

“From the supply chain perspective, blockchain can be an enabler of trust between trading partners as well as with consumers,” said Ajay Chidrawar, vice president of global product management and customer success. “From the farm to the shelf, consumers can now see the full lifecycle of the garment with blockchain technology. Consumers are going from blind trust to a full understanding of the journey of that garment. With blockchain, sustainability and compliance of an item can be tracked on the raw materials and manufacturing processes.”

CROSS-BORDER PAYMENTS

[Binkabi](#), a cross-border agricultural trading platform, is tapping a blockchain solution from [Sweetbridge](#) to develop a system for fair commodity trading in underdeveloped countries, where access to banking services and working capital is a problem.

IBM also recently announced a new [blockchain banking solution](#) that allows financial institutions to more quickly and cost effectively process payments across international borders.

FOOD SAFETY

[IBM](#) is partnering with [food suppliers](#) including Dole, Nestlé, and Walmart to better regulate food safety using blockchain. In the global food supply chain industry, this means all growers, suppliers, processors, distributors, retailers, regulators, and consumers can gain permissioned access to information about the origin and state of food in their transactions. All members of the ecosystem can use the blockchain network to trace contaminated foods to their source in a short amount of time to ensure that they are quickly removed from store shelves.

The [World Wildlife Fund \(WWF\)](#) is also using blockchain to better track seafood.

“Consumers are increasingly calling for fully traceable seafood that does not come from illegal fisheries or those that engage in human rights abuses,” said Bubba Cook, WWF Western Central Pacific Tuna Program manager. “Wholesale and retail seafood buyers are asking for improvements in transparency and traceability to

reduce the risk of their brands being associated with dubious and illegal activities. Layered into the real-time information coming from other electronic technology platforms, blockchains can provide unprecedented supply chain transparency and traceability that retailers and consumers want.”

HUMANITARIAN CRISES

The United Nations (UN) is exploring how blockchain can be used internally and externally to address ongoing humanitarian issues, such as child trafficking, according to Mahrinah von Schlegel, executive director of the nonprofit Embassy2.0. The UN is currently using blockchain across 16 agencies, including the World Food Program (to help refugees purchase food with only an eye scan) and the Office for the Coordination of Humanitarian Affairs (to improve donor financing, securing and monitoring supply chains, and data protection).

Microsoft and Accenture also [recently announced](#) a partnership to use blockchain technology to provide a legal form of identification for 1.1 billion people worldwide as part of the global public-private partnership ID2020.

JEWELRY

Ethically sourced jewelry company [Brilliant Earth](#) is partnering with [Everledger](#) to use blockchain to track and trace the provenance of diamonds and other gemstones to ensure that they are conflict free.

18 NEW IT JOBS CREATED BY BITCOIN AND BLOCKCHAIN

BY ALISON DENISCO RAYOME

As bitcoin and blockchain are poised to revolutionize many businesses, employers and job candidates alike are investigating how cryptocurrency-related positions could be of use to their business.

Searches for jobs mentioning blockchain, bitcoin, or cryptocurrency jumped more than 1,000% since November 2015, according to new data from job search site [Indeed](#). Job postings on Indeed specifically mentioning blockchain, bitcoin, or cryptocurrency in their search also increased by 621% in that time.

“While the number of opportunities and searches is still quite small, Indeed data shows that companies are increasingly seeking experts to focus on this new technology—and job seekers have been quick to react,” said Terence Chiu, vice president of product at Indeed. “It remains to be seen whether the rapid growth in this field will continue, and it’s worth noting that these are specialized roles that can be hard to fill. However, it’s certainly a field worth watching in the near future as both job seekers and employers seize the opportunity.”

Here are 18 jobs that currently mention blockchain, bitcoin, or cryptocurrency, posted on Indeed:

- Senior software engineer, cryptocurrency
- Cryptocurrency analyst
- Cryptocurrency developer
- DevOps engineer—Bitcoin enthusiast
- Analyst (cryptocurrency)
- Cryptocurrency trader
- Project manager—cryptocurrency
- Product manager—Cryptocurrency
- Certified cryptocurrency specialist positions—direct sales
- Cryptocurrency mining technician
- COO (cryptocurrency)
- Direct sales associate—cryptocurrency
- Systems engineer (trading cryptocurrency)

- Data scientist (cryptocurrency)
- Cloud engineer with Bitcoin protocol / blockchain
- Bitcoin full-stack developer
- Cryptocurrency mining lead
- Cryptocurrency research analyst (internship)

Using [Indeed Prime](#), the site could see what employers have been searching for and contacting candidates with bitcoin or blockchain skills. These included the following companies:

- Allstate
- Capital One
- Deloitte
- ESPN
- Electronic Arts
- Evernote
- GEICO
- Instacart
- JP Morgan Chase
- Match.com
- Philips
- Priceline
- Pure Storage
- Thumbtack
- Twilio
- Uber
- eBay

It's uncertain exactly how blockchain and cryptocurrencies will affect the enterprise, but [experts say](#) the technologies are poised to disrupt industries including finance, shipping, and law.

FIVE COMPANIES USING BLOCKCHAIN TO DRIVE THEIR SUPPLY CHAIN

BY OLIVIA KRAUTH

Blockchain, the ledger technology that supports Bitcoin and other cryptocurrencies, is being increasingly adopted for enterprise use. Since it creates and maintains a permanent transcript of an item's transactions, blockchain technology can be helpful for tracking a company's supply chain. Using the emerging technology instead of past methods could be more efficient and accurate, saving businesses time and money.

Here are five companies experimenting with using blockchain to drive their supply chain.

1. WALMART

Using blockchain, Walmart employees can track some products back to their roots—literally. After scanning mangoes or a couple of dozen other products with the store's app, employees can see which farm the fruit came from and where it's stored in the backroom, according to the *Wall Street Journal*. The technology could help customers understand where their food comes from and could streamline the restocking process.

2. MAERSK

The world's largest shipping company completed its [first test](#) of blockchain technology in March 2017, looking at how it could help manage its cargo. In the test, Maersk, Dutch customs, and US Homeland Security were all able to remotely access data about the cargo, suggesting the technology may streamline and secure international shipping.

3. BRITISH AIRWAYS

The airline tested using blockchain to manage data about flights between London, Geneva, and Miami in 2017, the *Wall Street Journal* said. Using one unchangeable history source, the airline hoped to reduce conflicting flight information coming from gate monitors, flight apps, and the airline's website.

4. UPS

The shipping company UPS joined the [Blockchain in Trucking Alliance](#) (BiTA) in November, hoping to push for increased transparency among all groups involved in the supply chain. The group is working to develop blockchain standards for the freight industry.

“In the future, blockchain standards and intercompany collaboration will support the logistics strategies that enable UPS customers to participate in global trade and finance,” UPS said in a [press release](#).

Currently, UPS is looking at how blockchain can be used in its customs brokerage business.

5. FEDEX

FedEx, another shipping giant, joined [BiTA](#) in February and has already launched a blockchain-powered pilot program to help solve customer disputes. The company hopes the program will clarify what data should be stored on the blockchain to best remedy customer issues. FedEx also hopes to use the technology to store records, vice president of strategic planning and analysis Dale Chrystie told [Coindesk](#).

HOW MICROSOFT IS POSITIONING ITSELF AS A LEADER IN ENTERPRISE BLOCKCHAIN ADOPTION

BY MARK KAELIN

In these early stages of blockchain's practical development, the discussion of the technology and its potential for business enterprises often revolves around cryptocurrency like Bitcoin and its derivatives. But limiting the discussion in that way is a mistake. The real potential for blockchain as a transformative and potentially disruptive technology lies within the more mundane and day-to-day realm of the basic business transaction.

By applying blockchain technology to business transactions, enterprises can establish more secure and more robust cybersecurity—theoretically. Blockchain technology, particularly when applied as a cybersecurity protocol, is still in a nascent state of development. Applying this technology in a practical way that all businesses can agree and count on is a challenge Microsoft is meeting head on.



IMAGE: MICROSOFT NEWS

BLOCKCHAIN CYBERSECURITY

To move the discussion forward and overcome the challenges in front of it, [Microsoft published](#) a comprehensive whitepaper that addresses the practicalities of blockchain as a cybersecurity technology. The company published [Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry](#) (PDF) to “deepen the cybersecurity policy dialogue among blockchain technology providers.” The whitepaper concentrates on the financial services industry, but the principles can be applied to almost any business transaction.

Microsoft's whitepaper emphasizes the use of permissioned blockchain models and explains in detail what such a technology would require in order to be implemented with confidence in a regulatory environment. For

the financial services industry, and any regulated industry, all security measures must be understood and agreed upon by both the enterprises making the transactions and the regulators charged with ensuring lawful compliance.

PERMISSIONED BLOCKCHAIN MODEL

Cryptocurrencies like Bitcoin follow a public blockchain model, which means any person with the technological capability can access the transaction ledger, propose the addition of new blocks (Bitcoins), and validate transactions by following the established protocols. This public access is why mining for new coins has become such a big business for speculators.

The permissioned blockchain model, on the other hand, restricts access to the transaction ledger to certain agreed-upon parties. Ideally, the parties with access to the ledger will use their true identities and be vetted for trustworthiness. Permissioned blockchains may be developed by a single party or by a consortium of companies. According to Microsoft's whitepaper, permissioned blockchains rely upon a governance structure to control access, apply and enforce rules, and respond to incidents, including cyberthreats.

BOTTOM LINE

In many ways, blockchain technology is similar to cloud computing a decade ago. The technology is on the cusp of becoming standard operating procedure for many enterprises, with many practical applications we have yet to imagine, much less implement. Enterprises just need some time to work out the kinks and become comfortable with the technology.

Microsoft's whitepaper is a preliminary step in the enterprise adoption process. By showing enterprises, specifically those operating in regulated industries, how blockchain technology can improve the security of their business transactions while maintaining regulatory compliance, Microsoft is looking to advance blockchain technology as a potential business solution.

Of course, this is important to Microsoft because blockchain technology is, by its nature, best implemented via cloud computing services like Azure. Blockchain technology requires a reliable and secure infrastructure that can be trusted by all parties accessing the blockchain ledger. Through Azure and its intelligent cloud services, Microsoft is positioning itself to be at the forefront of the practical development of blockchain technology.

IS BLOCKCHAIN OVERHYPED?

BY OLIVIA KRAUTH

As Bitcoin and other cryptocurrencies grow in popularity, the technology beneath it—blockchain—grows as well. Essentially a permanent, unchangeable ledger of transactions, blockchain has several potential enterprise uses outside of currency. Although it is a relatively young technology, it has been the center of experiments in multiple industries, including [energy](#), [manufacturing](#), and [banking](#).

Even companies outside of those industries are looking into ways to digitally transform their business, or parts of it, using blockchain. Singapore Airlines is moving its frequent flyer program to a blockchain-enabled [virtual wallet](#), and shipping giants FedEx and UPS are looking at ways to increase transparency in the shipping industry and track their supply chains using blockchain.

But could the technology be overhyped? A [December Gartner report](#) found that only 10% of companies will achieve digital transformation by 2022 by using blockchain, adding that the technology is more a long-term investment than a one-size-fits-all quick fix.

TechRepublic talked to five experts and practitioners to get their take on blockchain value. The consensus: Some aspects or early uses are overhyped, but the technology itself is not.

Here are their full explanations.

1. Michela Menting, digital security research director, [ABI Research](#)

“I don’t believe blockchain is overhyped; Bitcoin may be, but not the underlying infrastructure on which it is built. The architecture is transformative in many ways, and especially the decentralization concept. The digital age has a tendency to enable revolutionary ideas; look at smartphones, online commerce, or social networking and the behemoths they created.

“Cryptocurrencies are just the first iteration of what blockchain is capable. The hype, the divisions, the furor around a first generation technology is certainly incredible; it is enough to belie arguments that it is simply a fad. As the technology itself matures, and new use cases are tested and tried, the value of blockchain will be difficult to deny. I think we are in for an exciting decade for blockchain!”

2. Martha Bennett, analyst, [Forrester](#)

“Yes, it’s definitely overhyped. My biggest fear is that the hype is going to be detrimental: As many have pointed out, the current approach is a bit like ‘When you’ve got a hammer, everything looks like a nail.’ This tech-led

approach is bound to lead to failed projects, which in turn will lead to disillusionment with the technology; but it's not the technology's fault when it's used in scenarios that either don't need a blockchain-based approach or where non-technology factors derail the project.

“Also, a lot of the headlines make it seem like the technology is a lot more mature than it is, and the projects more advanced than they are; ultimately, this can only lead to disappointment.”

3. Michael Fauscette, chief research officer, [G2 Crowd](#)

“I don't think [blockchain is overhyped]. It's a reasonable, simple, and yet elegant way to verify transactions, and has many uses that add quite a bit of value.”

4. Kat Kuzmeskas, founder, [SimplyVital Health](#)

“Some aspects of the blockchain are overhyped, some are underhyped. Right now, there's been a lot of focus on the amount of money pouring into the blockchain space. But what's really a much more interesting story is the number of talented people who are just starting to identify and work on huge societal problems that the blockchain can help disrupt—like healthcare. We're just on the cusp of radical breakthroughs that can begin to attack some of the most challenging problems of our day.”

5. Richard Ma, founder, [Quantstamp](#)

“The blockchain technology itself is underhyped—because not a lot of people actually understand the technology. There are a lot of discussions around the overall phenomenon—but very little interest in new fields that the technology can be applied in. The technology is still very early stage, but it has the potential to change transparency in government and NGOs and create a transaction layer for individuals on a global scale.”

HOW BLOCKCHAIN COULD SAVE LIVES BY GETTING MEDICINE WHERE IT'S NEEDED

BY NICK HEATH

Blockchain may be famous as the technology that underpins Bitcoin, but it could also play an important role in transforming healthcare.

What makes blockchain so potentially useful to the health industry is that it offers a decentralized database that is immutable and unforgeable.

According to Jim Nasr, who until recently was chief software architect at the Centers for Disease Control and Prevention (CDC), the guarantees offered by that database could help tackle one of the most pressing issues in the field: stamping out counterfeit drugs.

“Counterfeit drugs are a real problem, the estimate for economic loss is about \$200bn, and of course, it’s more than financial, we’re also talking about lives being lost,” he said, speaking to TechRepublic at the London Blockchain Week summit in January.

“Somewhere up to about a million people have died because of counterfeit drugs, because they think they’re getting some aspirin but the reality is some low-quality mishmash.”

A number of startups, such as FarmaTrust, already offer tracking systems based on blockchain designed to keep counterfeit drugs out of the supply chain.

However, just using blockchain to improve the efficiency of the pharmaceutical supply chain by automating manual processes could have a profound impact, according to Nasr, who is now VP for technology & innovation at health tech firm Synchronix.

“The inefficiency of the drug supply chain leads to two major problems. One is that it increases the cost of drugs; the other is that it increases the time it takes for a compound to go from discovery all the way to being approved by the FDA in the US,” he said.

What makes blockchain so potentially useful to the health industry is that it offers a decentralized database that is immutable and unforgeable.

“So if it’s a drug that’s very important for saving lives, let’s say for instance a cancer drug, if it’s taken 10 years to go from conception to being approved, well if that time could be cut down, especially through [eliminating] unnecessary and manual processes, and finding more efficient ways of doing things, that could save lives. That drug could get to market faster; it could be approved faster.”

Using blockchain technologies to improve the quality of the supply chain is what Nasr has focused on, although he says most of the projects to use blockchain at the CDC are still in the proof-of-concept phase.

Among these trial projects is an attempt to use blockchain to improve information sharing by using decentralized blockchain-based databases to share information about health crises and threats between a wide range of public health agencies, hospitals, and pharmacies.

However, using blockchain to handle identifiable patient information will be far more challenging he said, due to the lack of standardized national systems for handling identity management.

UNIVERSITIES ARE ADDING BLOCKCHAIN CLASSES TO HELP CLOSE THE ENTERPRISE TECH SKILLS GAP

BY ALISON DENISCO RAYOME

Blockchain is poised to revolutionize the enterprise across a number of industries, but knowledge of how the technology actually works remains lacking from both a tech and business perspective. Universities worldwide are beginning to step up and try to fill the gaps, teaching students and collaborating with companies on best use cases for the blockchain to enhance security and productivity.

For those unfamiliar, blockchain is a public ledger technology that uses digital signatures and cryptographic hashing to provide a record of secure transactions that can't be altered. It is also the technology that allows Bitcoin and other digital currencies to be open, anonymous, and secure.

“Blockchain adoption is in the very, very early stages,” said Martha Bennett, principal analyst at Forrester. “There is a lot of interest, and a lot of companies are experimenting. But there are comparatively few that really realize that you need to take a long term view to it. This is not just about building a faster force, it's about transforming the way in which we do things.”

As demand for professionals skilled in blockchain technologies begins to skyrocket, a number of universities in the US—including Stanford, MIT, and University of California-Berkeley—have begun offering courses in either blockchain or cryptocurrencies. Many online tutorials and massive open online courses are also available.

Searches for jobs mentioning blockchain, bitcoin, or cryptocurrency jumped more than 1,000% since November 2015, according to Indeed, and several new IT jobs have been created around the technologies.

“It's good that academia is beginning to be more interested, because a lot of companies have jumped into technologies like this that haven't been properly scientifically reviewed or researched,” Bennett said. Many current blockchain practitioners are self-taught and came from fields including cryptography, distributive systems, and advanced mathematical modeling, she added.

YOUNG TECHNOLOGY, YOUNG TALENT

In 2016, [Blockchain at Berkeley](#) launched as an undergraduate organization that now offers two courses to students: Blockchain Fundamentals is a generalized course for students from any major to take, and Blockchain for Developers is a deeper dive class for students with coding abilities to turn that basic knowledge into actionable skills.

Interest in the courses has increased, likely in part due to the Bitcoin price spikes hitting the news, said Nick Zoghb, a junior computer science major at UC Berkeley and one of the undergraduate instructors of the blockchain course.

“Despite the various dips that have been occurring over the recent weeks in pricing, we still see an increase in interest in blockchain,” Zoghb said. “Currently it’s a buzzword, and many people even outside of the electrical engineering and computer science departments here at Berkeley are seeking out more resources to be able to study it and find out what blockchain is.”

The developers course is capped at 80 students, while the fundamentals course is limited to 200 students, but the number of applicants to each course far exceeds the number of available spots, Zoghb said.

Universities across the globe reach out to Blockchain at Berkeley on a weekly basis to ask for advice on course design, he said, so it’s likely that similar courses will pop up worldwide in the near future. Berkeley is also launching an edX course to bring its classes to a wider audience.

However, Bennett said that universities will need to take care in creating these courses.

“We need to distinguish people just putting on courses because it’s a hot topic, and those doing serious research.” Some curricula are so high-level that it’s almost meaningless, she said.

Course curricula will need to be updated regularly, as the technology is in a rapid state of change, Zoghb said. “In the past there have been a number of security issues with blockchain development. Remaining up to speed with the developments in the space really benefits everyone involved.”

Blockchain at Berkeley also consults with companies to develop strategic approaches to implement blockchain technologies. But Zoghb said that when working with a business, it’s important to first ask whether blockchain is the best solution, because many others exist that are more established.

“One of the pillars of our education program is tackling blockchain, especially enterprise-facing blockchain solutions from a pragmatic standpoint,” Zoghb said. “That is to say that one must be incredibly vigilant and have knowledge of the already existing solutions that are non-blockchain related.”

**“In the past there have been a number of security issues with blockchain development. Remaining up to speed with the developments in the space really benefits everyone involved.”
— Nick Zoghb**

With a young technology like blockchain, most of the people who are involved in the space also tend to be young. For example, Blockchain at Berkeley is one of the largest academic organizations focused on this space right now, and it is made up entirely of undergraduates, Zoghbi said, many of whom have gone on to become experts in the field.

Bennett said that while younger developers tend to be creative, they lack enterprise experience, such as how to harden applications for business purposes. She encouraged academic institutions to focus on deep research to fully utilize the concept for new business models.

“There is a big gulf between successful proof of concept and actual deployment,” Bennett said, with issues arising around user interface, key management, and SLAs. “If that is something that can be picked up in some of these courses from people who have done research, that I would greatly welcome.”

WHY USING BLOCKCHAIN TO TRACK COBALT MINING COULD LEAD TO MORE ETHICAL SMARTPHONES

BY OLIVIA KRAUTH

The Democratic Republic of Congo is utilizing blockchain technology to track cobalt from its artisanal mines to the smart device it ends up in, according to a [Reuters report](#). More conflict materials—elements mined from warring areas or with child labor—have been used in smartphones and other devices using lithium-ion batteries. With [millions dying](#) in these areas, tech giants are looking for ways to avoid human rights concerns while still getting the materials they need.

The plan is designed to make sure the cobalt isn't mined by children in a time when more tech giants are under pressure to ensure that their products aren't enabled by child labor, Reuters said. Blockchain, the emerging technology behind [Bitcoin](#), may be the key to understanding where the cobalt comes from and may reduce reliance on child labor.

Congo holds more than half the world's cobalt reserves, making it the largest producer of the in-demand element.

The blockchain monitoring technique would begin at the point of production: Congo's artisanal mines. Each sealed bag of cobalt will receive a digital tag at the mine, entered into the system via mobile phone, Reuters said. When the buying begins, each trader will update the blockchain throughout the process until it reaches its end destination. The blockchain record will be unforgeable.

Blockchain is already used for tracking in the diamond industry, but the cobalt industry can be more difficult to maneuver. Frequently set up informally and located in remote areas, the mines' output can be hard to track. The country's "opaque legal system" and conflicts add issues, Reuters said.

Child-mined cobalt could also be added to a bag of regular cobalt before the tag gets applied.

Still in its relatively early stages, blockchain may have a transformative impact on several industries, including [manufacturing](#) and [banking](#). Companies and organizations are using the technology in other unique ways, including marking counterfeit drugs and finding ways to use it as an [ID](#). Some universities are even adding blockchain studies to the course catalog.

MICROSOFT LAYS OUT PLANS FOR BLOCKCHAIN-BASED DIGITAL IDS

BY ALISON DENISCO RAYOME

Over the past year, Microsoft has made a number of investments in using blockchain and other distributed ledger technologies to create new types of secure digital identities. Now the company has described its roadmap for the continuing use of these technologies to improve the lives of refugees and others who lack identification.

“Each of us needs a digital identity we own, one which securely and privately stores all elements of our digital identity,” Ankur Patel, principal program manager in the Microsoft Identity Division, said in a [blog post](#). “This self-owned identity must be easy to use and give us complete control over how our identity data is accessed and used.”

In January, Microsoft officially joined global public-private partnership ID2020 as a founding member, committing \$1 million to the initiative to help develop a secure, portable, blockchain-based form of digital identity, according to a [blog post](#) from Peggy Johnson, Microsoft executive vice president of business development.

Microsoft and Accenture [first announced](#) a partnership to use the technology to provide a legal form of identification for 1.1 billion people worldwide as part of ID2020 back in June 2017. The two tech giants developed a prototype that taps Accenture’s blockchain capabilities and runs on Microsoft Azure.

The tech tool uses a person’s biometric data, such as a fingerprint or iris scan, to unlock the record-keeping blockchain technology and create a legal ID. This will allow refugees to have a personal identity record they can access from an app on a smartphone to receive assistance at border crossings or to access basic services such as healthcare.

Microsoft’s goal is to start piloting ID2020 solutions in the coming year, beginning with refugee populations, Johnson said.

Patel described the best practices the company has learned from its decentralized identity work, including the need to own and control your identity. While users today grant broad consent to apps and services to collect, use, and retain their information, they need a better way to take ownership of their identity. “After examining decentralized storage systems, consensus protocols, blockchains, and a variety of emerging standards we believe blockchain technology and protocols are well suited for enabling Decentralized IDs (DID),” he said.

Users also need a secure, encrypted digital hub that can interact with their data while honoring their privacy and control, he said. Apps and services must be built with the user at the center—and DIDs and ID hubs can help developers access user information while reducing legal and compliance risks.

As a next step, Microsoft plans to add support from Decentralized Identities into Microsoft Authenticator, which will act as a User Agent to manage identity data and cryptographic keys. “In this design, only the ID is rooted on chain,” Patel said. “Identity data is stored in an off-chain ID Hub (that Microsoft can’t see) encrypted using these cryptographic keys.”

With this capability, apps and services will be able to interact with a user’s data using a common messaging conduit by requesting their consent. “Initially we will support a select group of DID implementations across blockchains and we will likely add more in the future,” Patel said.

NINE REASONS TO BE CAUTIOUS WITH BLOCKCHAIN

BY JOE MCKENDRICK

Is blockchain—the network of global online ledgers—really secure? Its proponents say yes, as it assigns transactions or smart contracts to an immutable ledger, verifiable by multiple parties. However, a recently published paper calls out some vulnerabilities that may subject blockchain entries to inefficiencies, hacking, and other criminal activity.

The paper, [published](#) by Xiaoqi Li, Peng Jiang, and Xiapu Luo (all with Hong Kong Polytechnic University), Ting Chen (University of Electronic Science and Technology of China), and Qiaoyan Wen (Beijing University), asserts that blockchains have several points of vulnerability that users need to be aware of.

As blockchain increasingly becomes part of business operations, there needs to be a closer examination of the potential security liabilities that come with this emerging technology. With the growth of the number of decentralized applications, “the privacy leakage risk of blockchain will be more serious,” Li and his co-authors said. “A decentralized application itself, as well as the process of communication between the app and Internet, are both faced with privacy leakage risks.” They urge greater adoption of techniques to address the challenge: “code obfuscation, application hardening and execution trusted computing.”

The researchers outlined these key known risk factors with blockchain.

1. BLOCKCHAIN EFFICIENCY

For starters, the efficiency of blockchains themselves may become overloaded with complex consensus mechanisms and invalid data. Li and his co-authors noted that the consensus mechanisms employed across the internet are computing resource hogs. For instance, the most popular consensus mechanism used in blockchain is Proof of Work (PoW), which the researchers call a “waste of computing resources.” They said there are efforts to develop more efficient and hybrid consensus mechanisms that combine PoW and Proof of Stake (PoS). In addition, blockchains will produce a lot of data—block information, transaction data, contract bytecode—that may be outdated and useless. “There are a lot of smart contracts containing no code or totally the same code in Ethereum, and many smart contracts are never executed after its deployment. An efficient data cleanup and detection mechanism is desired to improve the execution efficiency of blockchain systems.”

2. 51% VULNERABILITY

Blockchain “relies on the distributed consensus mechanism to establish mutual trust. However, the consensus mechanism itself has 51% vulnerability, which can be exploited by attackers to control the entire blockchain. More precisely, in PoW-based blockchains, if a single miner’s hashing power accounts for more than 50% of the total hashing power of the entire blockchain, then the 51% attack may be launched. Hence, the mining power concentrating in a few mining pools may result in the fears of an inadvertent situation, such as a single pool controls more than half of all computing power.”

3. PRIVATE KEY SECURITY

“When using blockchain, the user’s private key is regarded as the identity and security credential, which is generated and maintained by the user instead of third-party agencies. For example, when creating a cold storage wallet in Bitcoin blockchain, the user must import his/her private key.” An attacker could “recover the user’s private key because it does not generate enough randomness during the signature process. Once the user’s private key is lost, it will not be able to be recovered. Since the blockchain is not dependent on any centralized third-party trusted institutions, if the user’s private key is stolen, it is difficult to track the criminal’s behaviors and recover the modified blockchain information.”

4. CRIMINAL ACTIVITY

“Through some third-party trading platforms that support Bitcoin, users can buy or sell any product. Since this process is anonymous, it is hard to track user behaviors, let alone subject to legal sanctions.” Frequent criminal activities with Bitcoin include ransomware, underground markets, and money laundering.

5. DOUBLE SPENDING

“Although the consensus mechanism of blockchain can validate transactions, it is still impossible to avoid double spending, or using the same cryptocurrency multiple times for transactions. The attacker can exploit the intermediate time between two transactions’ initiation and confirmation to quickly launch an attack.”

6. TRANSACTION PRIVACY LEAKAGE

“Unfortunately, the privacy protection measures in blockchain are not very robust,” Li and his co-authors said. “Criminal smart contracts can facilitate the leakage of confidential information, theft of cryptographic keys, and various real-world crimes (murder, arson, terrorism, etc.)”

7. VULNERABILITIES IN SMART CONTRACTS

“As programs running in the blockchain, smart contracts may have security vulnerabilities caused by program defects.” For example, one study found that 8,833 out of 19,366 [Ethereum](#) smart contracts are vulnerable to bugs such as transaction-ordering dependence, timestamp dependence, .mishandled exceptions, and .re-entrancy vulnerability.”

8. UNDER-OPTIMIZED SMART CONTRACTS

“When a user interacts with a smart contract deployed in Ethereum, a certain amount of “gas” is charged. Gas can be exchanged with “Ether,” which is the cryptocurrency in Ethereum. This results in “useless-code related patterns” and “loop-related patterns,” leading to “dead code, opaque predicate, and expensive operations in a loop.”

9. UNDER-PRICED OPERATIONS

“Ethereum sets the gas value based on the execution time, bandwidth, memory occupancy and other parameters. In general, the gas value is proportional to the computing resources consumed by the operation. However, it is difficult to accurately measure the consumption of computing resources of an individual operation, and therefore some gas values are not set properly. For example, some IO-heavy operations’ gas values are set too low, and hence these operations can be executed in quantity in one transaction. In this way, an attacker can initiate a Denial of Service attack on Ethereum.”

CREDITS

Global Editor in Chief

Jason Hiner

Editor in Chief, UK

Steve Ranger

Managing Editor

Bill Detwiler

Editor, Australia

Chris Duckett

Senior Features Editors

Jody Gilbert

Mary Weilage

Senior Editor

Conner Forrest

Senior Writers

Dan Patterson

Teena Maddox

Chief Reporter

Nick Heath

Staff Writer

Alison DeNisco Rayome

Associate Editor

Amy Talbott

Multimedia Producer

Derek Poore

Associate Social Media Editor

Leah Brown

Cover image: iStock/ monsitj**ABOUT TECHREPUBLIC**

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Copyright ©2018 by CBS Interactive Inc. All rights reserved. TechRepublic and its logo are trademarks of CBS Interactive Inc. ZDNet and its logo are trademarks of CBS Interactive Inc. All other product names or services identified throughout this article are trademarks or registered trademarks of their respective companies.