Blockchain isn't a household buzzword, like the cloud or the Internet of Things. It's not an in-your-face innovation you can see and touch as easily as a smartphone or a package from Amazon. But in a world where anyone can edit a Wikipedia entry, blockchain is the answer to a question we've been asking since the dawn of the internet age: How can we collectively trust what happens online?

Every year we run more of our lives—more core functions of our governments, economies, and societies—on the internet. We do our banking online. We shop online. We log into apps and services that make up our digital selves and send information back and forth. Think of blockchain as a historical fabric underneath recording everything that happens—every digital transaction; exchange of value, goods and services; or private data—exactly as it occurs. Then the chain stitches that data into encrypted blocks that can never be modified and scatters the pieces across a worldwide network of distributed computers or "nodes."


Think about a blockchain as a distributed database that maintains a shared list of records. These records are called blocks, and each encrypted block of code contains the history of every block that came before it with timestamped transaction data down to the second. In effect, you know, chaining those blocks together. Hence blockchain.

A blockchain is made up of two primary components: a decentralized network facilitating and verifying transactions, and the immutable ledger that network maintains. Everyone in the network can see this shared transaction ledger, but there is no single point of failure from which records or digital assets can be hacked or corrupted. Because of that decentralized trust, there's also no one organization controlling that data, be it a big bank or a tech giant like Facebook or Google. No third-parties serving as the gatekeepers of the internet. The power of blockchain's distributed ledger technology has applications across every kind of digital record and transaction, and we're already beginning to see major industries leaning into the shift.

First up are the big banks and tech giants. Big business will always drive innovation, and the rise of blockchain-based smart contracts (read on for a deeper explanation) turns blockchain into a middleman to execute all manner of complex business deals, legal agreements, and automated exchanges of data. Companies such as Microsoft and IBM are using their cloud infrastructure to build custom blockchains for customers and experiment with their own use cases, like building a worldwide food safety network of manufacturers and retailers. On the academic side, researchers

are exploring blockchain applications for projects ranging from digital identity to medical and insurance records.

At the same time, dozens of startups are using the technology for everything from global payments to music sharing, from tracking diamond sales to the legal marijuana industry. That's why blockchain's potential is so vast: When it comes to digital assets and transactions, you can put absolutely anything on a blockchain. A host of economic, legal, regulatory, and technological hurdles must be scaled before we see widespread adoption of blockchain technology, but first movers are making incredible strides. Within the next handful of years, large swaths of your digital life may begin to run atop a blockchain foundation—and you may not even realize it.

## Beyond Bitcoin

Blockchain is the data structure that allows Bitcoin (BTC) and other up-and-coming cryptocurrencies such as Ether (ETH) to thrive through a combination of decentralized encryption, anonymity, immutability, and global scale. It's the not-so-secret weapon behind the cryptocurrency's rise, and to explain how blockchain came to be, we have to begin briefly with the legacy of Bitcoin.

On Oct. 31, 2008, Bitcoin founder and still-mysterious Satoshi Nakamoto (a pseudonym) published his famous white paper introducing the concept of a peer-to-peer (P2P) electronic cash system he called Bitcoin. The Bitcoin blockchain launched a few months later on Jan. 3, 2009.

For Jeff Garzik, it started the way many a buzzy idea in the tech community has over the years: with a post on "news for nerds" and OG tech aggregator Slashdot.org. Garzik is the CEO and cofounder of enterprise blockchain startup Bloq, but has spent years as a Bitcoin core developer. He was also recently elected to the Board of Directors of The Linux Foundation (as the first member with a blockchain and cryptocurrency background).

In July 2010, Garzik was working on Linux at enterprise software company Red Hat when what he calls "The Great Slashdotting" occurred. One viral post introduced programmers, investors, and tech nerd-dom at large to the concept of Bitcoin, and by extension, to blockchain. Garzik had always been fascinated with the goal of making seamless digital payments work on a global scale and across borders. When he realized how Bitcoin's underlying technology worked, he said it "knocked him on his bum."

"I had already thought to myself about how someone might create a decentralized version of PayPal. When Elon [Musk] and Peter Thiel and the other founders created PayPal, they had this vision of a global ledger that could easily and cheaply add entries between users like a database entry. That vision met reality with banking laws and cross-border friction, with legal hurdles and regulations not only in the U.S. but around the world. It made that kind of decentralized global currency impossible, or so we thought.

"Bitcoin turned all of that on its head," Garzik went on. "From an engineering perspective, the proof of work was this very elegant way to elect a leader, the block creator, in this decentralized and potentially adversarial system. Bitcoin layered on top of that engineering a set of economic

and game-theory incentives that paid you in the script of the system itself, creating this virtuous cycle where it's in your best economic interest to to follow the consensus rules and create the longest, strongest chain possible. I didn't realize until that post on that day how elegantly it could be done."

It's important to understand why Bitcoin and blockchain are not the same thing. In Garzik's TEDx Talk (above), he described Bitcoin as "an organism." It has layers, like other software. On top of the public Bitcoin blockchain sits billions of dollars worth of cryptocurrency, but beneath that is a ledger just like any other blockchain. That decentralized ledger technology, and its myriad potential uses for securely transferring data and digital assets over the internet, is the subject of this feature. For a deeper dive into the nuances of cryptocurrencies like Bitcoin and Ethereum and the complex political dynamics at work in those communities, check out our explainer on why blockchains fork.

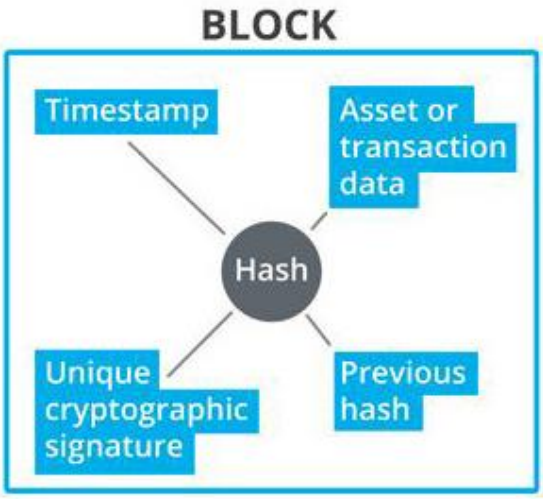
Garzik said Bitcoin was just the first demo application of what blockchain can do. In this case, it built a monetary revolution on the back of an all-seeing ledger, one that's everywhere and nowhere at once, and gave the cryptocurrency its power.

## Blockchain for Beginners

People often get bogged down in technological complexity when trying to understand blockchain, but the basic concept is a simple and universal one. We have facts and information we don't want accessed, copied, or tampered with, but on the internet, there's always a chance it could be hacked or modified. Blockchain gives us a constant—a bedrock we know won't change once we put something on it and where a transaction will be verified only if it follows the rules.

The Nakamoto white paper explains the basics of "mining" data into a block, then using a hash (a time-stamped link) to chain those blocks together across a decentralized network of "nodes" that verify each and every transaction. The other key innovation in the white paper is using what's known as the proof-of-work (PoW) model to create distributed "trustless" consensus and solve the double-spend problem (ensuring cryptocurrency isn't spent more than once).

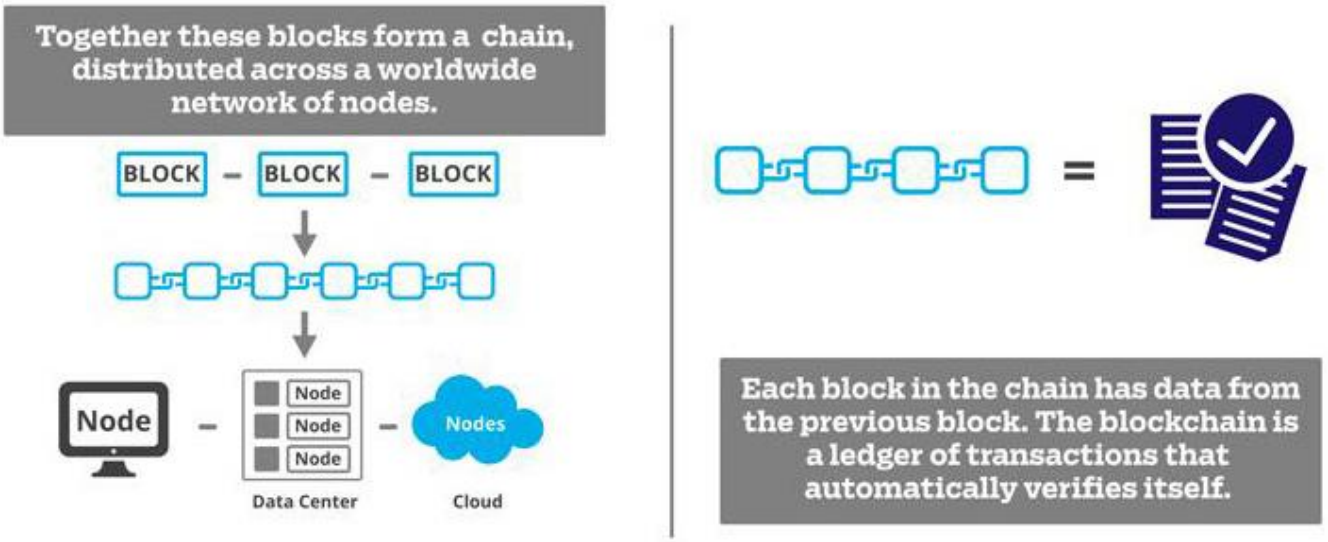
A "trustless system" doesn't mean it's a system you can't trust. Quite the opposite. Because the blockchain verifies each transaction through PoW, this means no trust is *required* between participants in a transaction. Where does the proof-of-work come from? The miners. A P2P network of Bitcoin "miners" generates PoW as they hash blocks together, verifying transactions that then go into the ledger.


In the 2016 book *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World,* authors Don and Alex Tapscott explain Nakamoto's Bitcoin model about as succinctly as one can:

"*Bitcoin or other digital currency isn't saved in a file somewhere; it's represented by transactions recorded in a blockchain—kind of like a global spreadsheet or ledger, which leverages the resources of a large P2P network to verify and approve each Bitcoin transaction. Each blockchain, like the [Bitcoin blockchain] is distributed: it runs on computers provided by volunteers around the world. There is no central database to hack. The blockchain is public: anyone can view it at any time because it resides on the network… and the blockchain is encrypted… it uses public and private keys (rather like a two-key system to access a safety deposit box) to maintain virtual security.*"

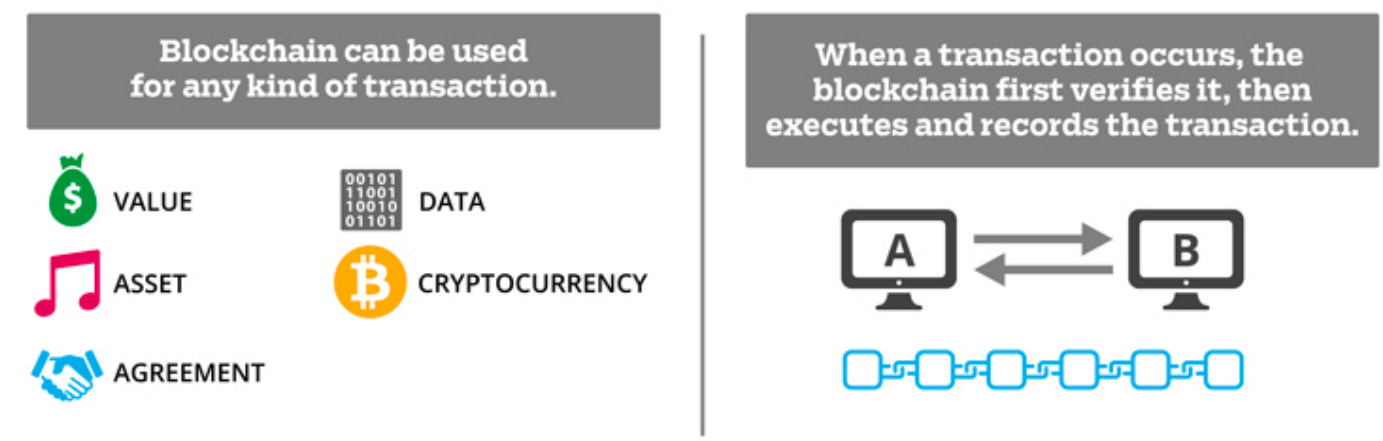
Note that nothing is completely unhackable, particularly when you don't use it as intended. Blockchain's security works not only because it's encrypted but also because it's also decentralized. Victims of the biggest blockchain breaches and cryptocurrency heists (Mt. Gox in 2014 and Bitfinex in 2016) were targeted and pilfered clean because they tried to centralize a decentralized system. Ethereum has seen a number of hacks and security incidents as well. Last year's DAO hack was traced to exploited loopholes in smart contracts written atop an established blockchain. More recently South Korea's largest Ethereum exchange was hacked, and an Israeli startup's initial coin offering (ICO) was hijacked when their website was hacked.




These issues all stemmed from vulnerabilities in systems connected to the blockchain, not within the blockchain itself. Blockchain's underlying security and encryption model is a sound one. How that security is executed is a story for another feature.

So we've explained how the network functions and how security works, but how do the blocks actually connect to one another? Why does a blockchain get stronger the longer it gets? Where does the immutability come in? The Tapscotts' explanation continues:

*"Every ten minutes, like the heartbeat of the Bitcoin network, all the transactions conducted are verified, cleared, and stored in a block which is linked to the preceding block, thereby creating a chain. Each block must refer to the preceding block to be valid. The structure permanently time-stamps and stores exchanges of value, preventing anyone from altering the ledger… so the blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. Like the World Wide Web of information, it's the World Wide Ledger of value… This new digital ledger can be programmed to record virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims, votes, provenance of food, or anything else that can be expressed in code."*




The concept of immutability is maybe the most crucial to understand when trying to wrap your head around blockchain and why it's important. An object that once created can never be changed has infinite value in our editable, ephemeral digital world.

Harking back to the "strength in numbers" principle, the more nodes a blockchain is distributed over, the stronger and more trusted it becomes. It's verification on top of verification to infinity. Bloq's Garzik talked about how the network effect of blockchain is key to its immutability, and why it's the reason the public Bitcoin blockchain is still the most popular and trusted blockchain out there:

"The immutability factor is very much dependent on the network effect," said Garzik. "You see that with Bitcoin very specifically. The cost of creating a new digital asset is essentially zero. Therefore you have to demonstrate an overwhelming amount of value in overcoming that network effect if you want to convince someone to switch away from the Bitcoin blockchain, which not only has a good track record but high security value from a technical perspective. Security and immutability are a direct function of the economics—how much investment there is in the ecosystem, and how many people are using it."

## Public vs. Private Blockchains

People within the industry talk a lot about public versus private blockchains. On a basic level, public blockchains are cryptocurrencies such as Bitcoin, enabling peer-to-peer transactions and, therefore, a revolution in seamless global payments. Interacting with public blockchains fundamentally requires tokens, and comes with its own rules of engagement, agreed upon by the P2P network. Private blockchains (those being built by distributed ledger consortium R3, for example) use blockchain-based application development platforms such as Ethereum or blockchain-as-a-service (BaaS) platforms such as those offered by Microsoft and IBM, running on private cloud infrastructure.

Brian Forde, Director of Digital Currency at the MIT Media Lab, likens public versus private blockchains to the relationship between an open-source technology, such as Linux, and companies like Red Hat that build on that tech for enterprise use. Public blockchains like Bitcoin were the open-source movement that started it all, and private blockchains such as R3 are taking that technology and commercializing it for businesses.

"A private blockchain is an intranet, and a public blockchain is the Internet. The world was changed by the Internet, not a bunch of intranets. Where companies will be disrupted the most is not by private blockchains but public ones," said Forde.

Bloq's Garzik echoed a similar thought when explaining the difference between public and private blockchains, but he uses the open-source analogy a bit differently. Bloq bills itself as a "Red Hat for blockchain" of sorts, but its platform is built atop the Bitcoin blockchain rather than a private or "permissioned" one. (Permissioned blockchains include an access control layer governing who can participate in the network.) Garzik's biggest question when looking at cloud providers and others building private blockchains and BaaS offerings is: Who's running that network?

"On the private and permissioned side, it's very much a question of who the referees are. I use that term specifically because what blockchains really provide is a neutral, level playing field for the execution of rules," said Garzik. "Those rules are applied to transactions that the actors create from that network. For Bitcoin, it's rules like the monetary supply; the number of transactions that can fit into a block. All of that forms the economic incentives and ultimately consensus rules that everyone in the network complies with and cross-checks to create this system of checks and balances.

"Some of the other blockchain networks, whether it's [open-source project] Hyperledger, Ethereum, or a bank chain [such as R3] are opening the question of trust and trust shifting," Garzik went on. "It's less about the technology, and much more about a rapid, near real-time adjudication of rules between actors on a network. That's what blockchains do."

Once you understand what a blockchain is and how it works, the next question an everyday tech user would have is how it'll affect them. If you're not a business that's building a blockchain-based product or service, why should you care? As Don Tapscott explained it in *Blockchain*

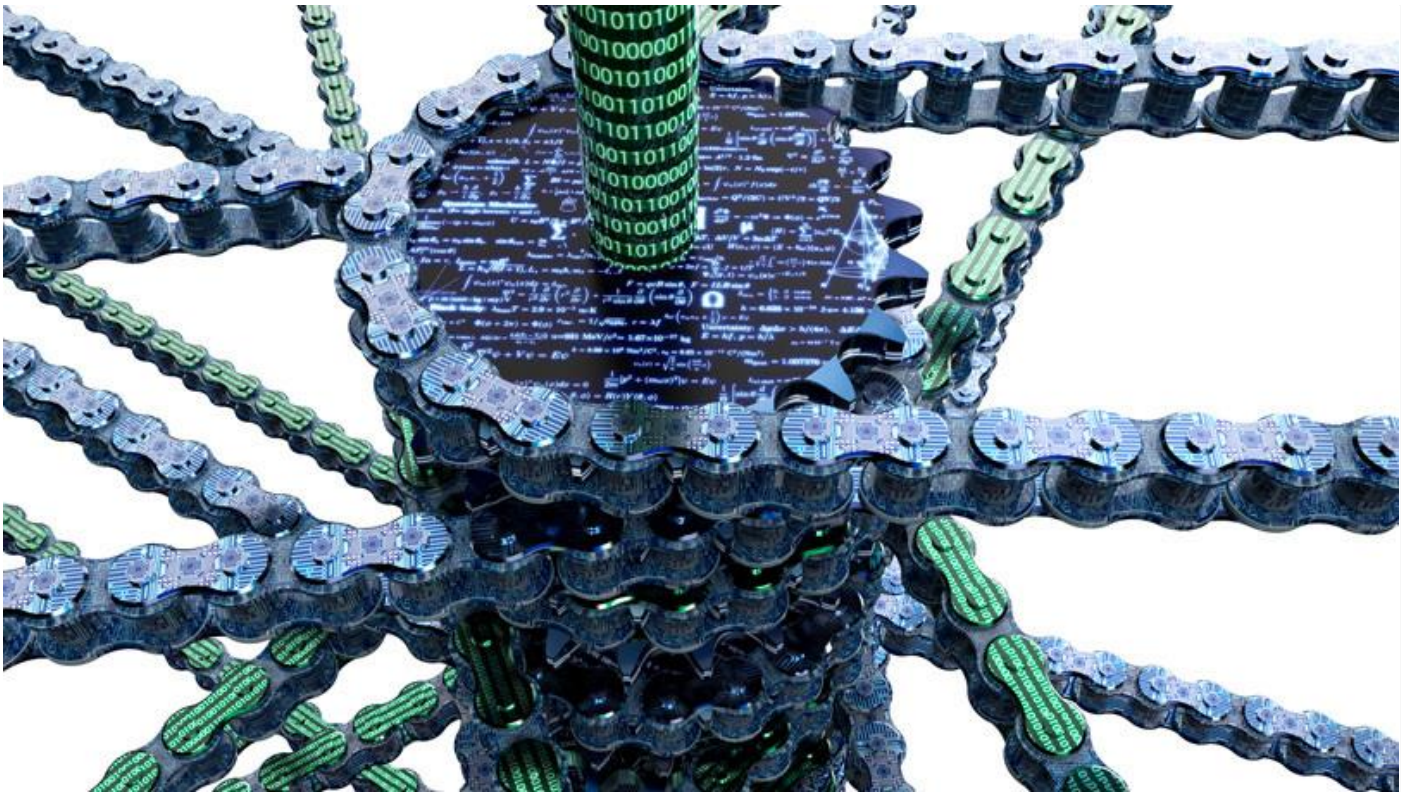
*Revolution* and in a 2016 TED Talk of his own, it's because blockchain brings us from the Internet of information into the "Internet of value." From his TED talk:

*"For the past few decades, we've had the Internet of information," says Tapscott. "When I send you an email or a PowerPoint file, I'm actually not sending you the original; I'm sending you a copy. That's great, and it has democratized information. But when it comes to assets; things like money, financial assets like stocks and bonds, loyalty points, intellectual property, music, art, a vote… sending you a copy is a really bad idea. If I send you $100, it's really important that I don't have the money afterward.*

*"Today, we rely entirely on big intermediaries; middlemen like banks, government, big social media companies, credit companies, and so on to establish trust in our economy," Tapscott continued. "These intermediaries perform all the business and transaction logic of every kind of commerce, from identification and authentication of people through to clearing, settling, and record-keeping… they capture our data, which means we can't monetize or use it to better manage our lives, and our privacy is being undermined… so what if there were not only an Internet of information, but an Internet of value. Some kind of vast, global, distributed ledger running on millions of computers and available to everybody, and where every kind of asset from money to music could be stored, moved, transacted, exchanged, and managed, all without powerful intermediaries."*

That, in a nutshell, is blockchain.

## What Are Smart Contracts?



If you think of blockchain as an operating system for data, then smart contracts are its killer app. Smart contracts add complex logic and rules atop a blockchain that can automate

traditional contract management and digitize the world around us the same way apps like Uber are automating away the need to wave your hand in the air to hail a cab.

You can't talk about the future of blockchain without explaining the role smart contracts will play. If the world is going to run on blockchain, much of it will rely on smart contracts to execute the data exchanges and program in rules to govern how each code-triggered agreement works. Smart contracts are also a flexible mechanism that can serve as the blockchain middleman for all manner of agreements and data exchanges, down to something as simple as verifying someone's identity to ensure they're of legal drinking age.

"Think about getting carded at a bar," said Jerry Cuomo, Vice President of Blockchain Technologies at IBM. "From an identity perspective, I can imagine a blockchain managing verification of a citizen's identity. A smart contract could ensure something like my daughter going out for her 21st birthday and the bouncer only being able to see her age, not her address. Blockchain could set up a centralized identity verification system that could make the world safer for dads like myself."

Identity management is an application to watch, but the list goes on and on. The Chamber of Digital Commerce, the leading trade association that represents the blockchain industry, runs the Smart Contracts Alliance. The Chamber and Alliance (in collaboration with Deloitte) released a white paper entitled "Smart Contracts: 12 Uses Cases for Business & Beyond" detailing a dozen broad areas and industries where smart contracts could change the game.

In a broad legal sense, smart contracts provide what Bloq's Garzik calls ""adjudication-as-a-service:" a real-time version of the court system that, for finance scenarios, can cut time on deal closings, banking and securities transactions, and even global trade finance from weeks or months to days, hours, or minutes. On the digital identity front, the white paper calls smart contracts a "user-centered Internet for individuals" giving users control over the data, digital assets, and online reputation associated with them. Blockchain also affords the ability to decide what personal data is and isn't shared with businesses—the same concept behind the driver's license analogy.

Beyond identity, the white paper also talks about how smart contracts can be applied to getting a mortgage and instantaneously processing auto-insurance claims. In the medical research field, they can serve as a mechanism to ensure better patient privacy in clinical trials while promoting more open data-sharing in the cancer research community. Another of the paper's use cases is land titling. Countries around the world, including Ghana, Georgia, and Honduras, that are typically rife with property fraud and land disputes are already implementing smart contracts to facilitate property transfers and land ownership.

Real-world smart contracts are also gaining traction in a few other interesting ways. Everledger is a blockchain-based fraud-detection system for valuable physical assets, particularly jewelry and

diamonds. It uses a hybrid blockchain that combines the Bitcoin blockchain with its own private blockchain to build smart contracts that certify physical diamonds. It combats the sale of conflict diamonds by keeping a transaction history for each gem.

"Everledger takes a diamond or a piece of art and hashes it to the blockchain," said MIT's Forde. "For something like a diamond ring, Everledger takes an image of it—like a unique diamond fingerprint—which can then be scanned against the blockchain to verify it's the same one."

Once you open the door of tracking and manage physical assets, smart contracts can tackle the whole supply chain. IBM and Walmart are even partnering in China to track the movement of pork (seriously) to keep people from eating tainted meat.

You can also use smart contracts for digital content such as music. Mycelia, a "collective of creatives, professionals and lovers of music" founded by musician Imogen Heap, is a blockchain-based protective ecosystem pushing smart contracts as a way for musicians to share free-trade music and to ensure the profits go back to the artists.

Mycelia is an example of blockchain and smart contracts' potential for digital rights management (DRM). Smart contracts in digital music files or other copyrighted material might enable artists to better sell directly to consumers without the need for labels, lawyers, or accountants, with royalties paid out automatically.

A sleeping giant in this conversation is the effect smart contracts could have on the Internet of Things. Think about all the data smart devices collect. Fitness trackers collect your body's vital statistics. Thermostats collect temperature data. Alexa has records of every search and request you've ever asked of her. If the IoT ran on a blockchain, and smart contracts governed that real-time data, it could create a whole new class of lending and other usage-based agreements, according to Erin Fonte, Head of the Financial Services Regulatory and Compliance Practice Group at corporate law firm Dykema.

"If you had smart and connected cars that could report back actual usage stats, you could tie pricing into real-time usage and have it automatically adjust over the length of your vehicle lease and financing," said Fonte.

Think about how connected devices enable mobile payments without traditional credit card swiping at the point of sale. Instead of swiping your card at a terminal, you touch a thumb to your iPhone to use Apple Pay. The automated payment system is authenticating individuals and providing verifiable legal proof of transaction authorization, just as a smart contract using those same two permissions—authorization and permission—in an IoT device can make a transaction legally enforceable against a buyer or seller, which is particularly applicable in machine-to-machine (M2M) communication.

"Amazon Dash buttons are a prime example," said Fonte. "It's one little branded button you stick in your house, and then you don't have to log onto Amazon to reorder. Just press the button, and it repeats its last order. For connected homes and cars, blockchain's ability to monitor, collect, and make sense of data for transactions will drive the ability for humans to authorize machines to carry out activities like this as agents. The next step is that you don't need a button. Manufacturers will create customer and end-user [smart contract] agreements on the back end. "Your washing machine will have that feature built into the product itself."

## How We Build a Blockchain-Based World

Blockchain is still in its infancy. Before we see widespread adoption on the scale the technology is capable of, a lot needs to happen. We must have buy-in from government (which in the U.S. means working state-by-state on policies and legislation). The industry has to clear a labyrinth of legal and regulatory hurdles before blockchain can power better banking, identity, records, or anything else requiring official documentation that now runs on legacy government systems or even (still) on paper.

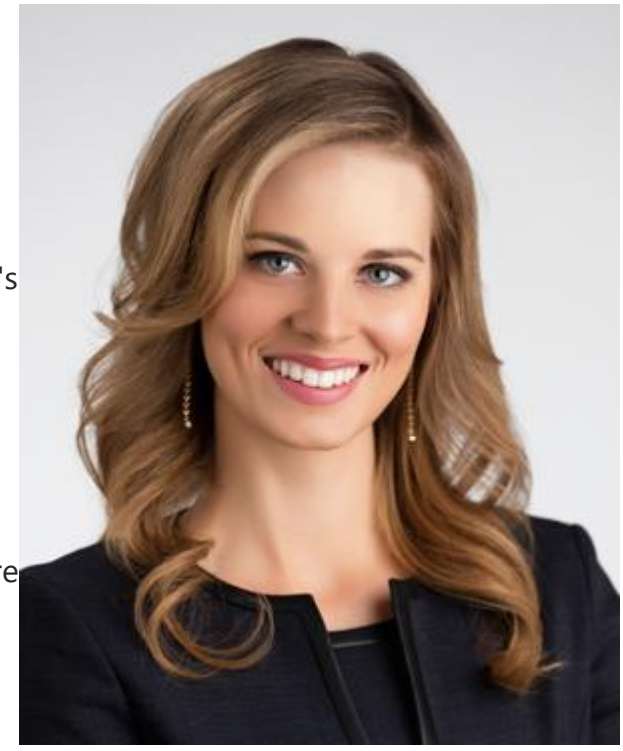
We also need open standards to tie the blockchain industry together. The most prominent coalition working to make that happen is the Hyperledger project. Hyperledger is an open-source initiative to create an open, standardized, and enterprise-grade distributed ledger framework and code base to be used across industries. Overseen by The Linux Foundation, its members include tech companies (Cisco, IBM, Intel, Red Hat, Samsung, VMware, and more), big banks (JPMorgan, Wells Fargo, and so on), blockchain startups such as Bloq, and a host of others. The project recently released the first production-ready version of Hyperledger Fabric as a foundation for building blockchain apps. Big blockhain players like Microsoft are beginning to get into the standardization game as well, with Redmond releasing its own Coco Framework to work with existing protocols and build more powerful governance and data confidentiality into private blockchains.

"The Linux Foundation is the key layer of governance for shepherding and maturing open-source products," said Garzik. "There are many blockchain peddlers out in the market right now, and one of the biggest pain points we see is incompatibility; a large bank that has merged 10 businesses over the past decade and has a lot of halfway-compatible internal legacy systems. That's where the foundation and Hyperledger really come to the fore. As young as the blockchain industry is, the kind of technical standards-making we need for interoperability has so far been absent."

Another important Hyperledger member is R3, the wealthy elephant in the room when it comes to blockchain standardization. R3 is a consortium dedicated to research and development of advanced distributed ledger technologies for global financial markets. It also represents most of the biggest banks and financial institutions on the planet: Barclays, Credit Suisse, J.P. Morgan, the Royal Bank of Scotland, UBS, Bank of America, Citi, Deutsche Bank, HSBC, Morgan Stanley, Wells Fargo, and a number of others.

We're already beginning to see the kind of blockchain-based international trading R3 is after. Last fall, the first cross-border transaction between banks using multiple blockchain applications took place between the Commonwealth Bank of Australia and Wells Fargo, resulting in a shipment of cotton to China from the United States. R3 is also becoming an example of how difficult standardizing blockchain can be. Goldman Sachs and Santander both left R3 in late 2016 in the midst of big-bank jockeying over control of a new funding round for the consortium. R3 is doing just fine, though. The consortium announced a new $107 round of funding in May.

As Ethereum and the value of the Ether currency have exploded in popularity in the past year, standardization efforts have emerged around its blockchain platform as well. The membership of the Enterprise Ethereum Alliance has amassed more than 150 enterprise organizations since its launch in February, spanning tech corporations, banks and financial institutions, blockchain and cryptocurrency startups, industries such as healthcare and energy, and even a few governments.



Few know the challenge of pushing for blockchain adoption better than Perianne Boring, president of the Chamber of Digital Commerce. The Chamber is currently engaged in lobbying and advocacy efforts in 14 states and counting. In North Carolina, the chamber's efforts helped pass the North Carolina Money Transmitter Act in July 2016, which updates the state's existing laws to include a defined "virtual currency."

Boring said the law is a big win for blockchain and digital currency but still only a drop in the bucket of patchwork state-by-state regulations and the even more muddled web of federal agencies. In the past year, Chamber representatives have testified at cryptocurrency regulation hearings in New Hampshire, lobbied regulatory proposals in New York and Washington states, and made official comments on virtual currency acts and regulatory frameworks from the Uniform Law Commission and the Conference of State Bank Supervisors (CSBS).

"How is digital currency supposed to be regulated? This is a huge national debate around how states can effectively regulate digital currency and money transmission, and every state has its own opinion and a completely different way of doing things," explained Boring. "New York says businesses need a separate digital currency license to operate in the state. North Carolina said that's way too complicated and regulatory overkill, and decided instead to amend their existing money transmission laws to incorporate digital currency. We prefer the latter approach."

Boring also stressed the importance of keeping blockchain technology and policy on the same page. The Chamber is also a Hyperledger member, and Boring said the Chamber will work to actively bring Hyperledger into policy discussions, to ensure lawmakers understand the pros and cons of regulations.

Yet as difficult as overcoming entrenched legacy systems and regulations can be, we already have a blueprint of how it can be done. Over the past two years, the state of Delaware has shown how governments can legislate, sanction, adopt, and implement blockchain technology to power core services.

As with much of the legislation, regulation, and business drivers behind blockchain, it starts with fintech (financial technology). More than a million companies and 66 percent of Fortune 500 companies are incorporated and legally headquartered in Delaware, in large part because of the state's largest export: uncertified shares (meaning the ability to own shares in a company without holding the actual stock certificate). In partnership with blockchain fintech company Symbiont, the Delaware Blockchain Initiative announced in 2016 will completely automate stock issuance and recordkeeping on a blockchain ledger.

'Before the Delaware Blockchain Initiative, there was no technological solution to support digital representation of share ownership," explained Symbiont CEO Mark Smith. "From what can only be described as a forward-thinking agenda from the state, they embraced that they could reimagine how to deliver their marquee service on a distributed ledger, using Symbiont's technology to create a new type of share and change the way a corporation works from now into the foreseeable future."

A little finance background: The genesis moment of a private equity is when you incorporate a company. As Smith explained, now companies will have the ability to carry that equity all the way from incorporation up to and including an initial public offering (85 percent of IPOs happen in Delaware), all via the blockchain, with complete financial transparency for state lawyers and regulatory agencies. The entire process will run automatically on smart contracts.

## Overstock Bets Big on Blockchain

E-commerce retailer Overstock.com became the first publicly traded company to issue stock on the blockchain this past December, selling 126,565 shares through its subsidiary, t0: the first-ever blockchain-based trading platform for stocks and securities. Overstock has been developing t0 for more than two years to serve as a distributed immutable ledger for capital markets.

Overstock CEO Patrick Byrne has called t0 a blockchain version of Wall Street, and in a Q&A with PCMag, the outspoken executive talked about how the platform works, making history with t0, and how blockchain could turn capital markets into *Game of Thrones*.

"I think what's going to happen is similar to what English common law did over a century ago. Blockchain is going to disrupt all kinds of legal work, notary publics, contracts, lawyers, judges, you name it," said Byrne. "You're going to start seeing open-source, self-executing contracts gradually improve over time. What the Internet did to publishing, blockchain will do to about 160 different industries. It's crazy."

Read our entire interview with Overstock CEO Patrick Byrne here.

Even greater implications lie in what the Delaware Blockchain Initiative is doing beyond digital shares. At the Consensus blockchain technology summit this past year, Delaware Governor Jack Markell gave a keynote speech announcing the initiative and laying out a blockchain roadmap for the next five years, including a new joint effort with Symbiont to digitize and store the entire Delaware Public Archives on a blockchain ledger in 2017.

Symbiont's Smith, who is also a co-chair of the Chamber of Digital Commerce's Smart Contracts Alliance, explained how Delaware is building cryptographic document control that will ultimately overhaul how city, county, and state municipalities share information that in many cases still exists on paper in filing cabinets. Smith's first conversation with Delaware officials was in October 2015, and between then and now, the state has gone from knowing nothing about blockchain to embracing it in its biggest export and mobilizing to push new legislation and initiatives around it.

"The state is completely reimagining how it stores and distributes public records to its citizens. Land and property titling, licensing, birth and death certificates, automobile VIN numbers, heavy machinery and luxury good registrations, all these things are being incorporated into Symbiont's technology stack behind the Delaware blockchain," said Smith. "Distributed ledger technology is not a silver bullet—it's not going to solve every problem—but it does solve some very big ones.

"When [Delaware] Governor Markell came out publicly announcing the initiative, he said he wanted to challenge us to use this powerful technology," Smith continued. "Delaware should serve as a blueprint for many other states, each of which could operate a node right next to Delaware and build critical mass and momentum from a government perspective that could lead to other nations joining in."

## Potchain: Where Blockchain Meets Marijuana

Medical and recreational marijuana is being legalized in more and more states across the U.S. This new, fast-growing sector of the economy presents challenges we haven't dealt with before, partly because even in states where it's legal, there are still a lot of things cannabis-related businesses can't do. Blockchain is helping fill in gaps for entrepreneurs, particularly when it comes to banking and legal protection.

Current federal banking regulations still preclude banks from doing business with cannabis companies, leaving them without a dedicated banking system. Tokken, a digital bank startup, gives cannabusinesses a bank account and blockchain-based transaction history that's linked to brick-and-mortar banking institutions and seed-to-sale systems, with Tokken as the middleman.

More interesting is what Medical Genomics is doing on the science side of the potchain. The life sciences company is mapping and sequencing the DNA of different cannabis strains, then storing and registering that info on the Bitcoin blockchain. The company lists this information on its public-facing Kannapedia strain database, but of far greater importance is how the company uses blockchain-based strain DNA as intellectual property (IP) protection for growers. The government makes it very difficult to obtain trademarks and patents for weed strains. But a blockchain provides irrefutable legal proof a grower can use to prove ownership of a strain if challenged by other growers or the pharmaceutical corporations that will ultimately enter the legal industry.

Check out the whole story for more on how blockchain is blazing a new trail for the legal cannabis industry.

# Welcome to Our Blockchain Future


The change blockchain represents to our digital world is tectonic. Blockchain is broad and coming to the fore on such a massive scale that explaining it often falls back on the abstract, rather than grounding it in the kind of foundational change the technology will have on the culture of how we interact online.

The Web 1.0 was a read-only Internet of static web pages. Web 2.0, where we are now, added dynamic user-generated content and the rise of social media. Web 3.0 has many definitions, but one of the most popular is that of connective intelligence: where the next generation of applications, data, concepts, and people are connected by an *unmediated* fabric where you don't need a trust broker like a bank or tech company in the middle to ensure privacy and security. In blockchain, we finally have the technology to power Web 3.0.

"The first four decades of the Internet brought us email, the World Wide Web, dot-coms, social media, the mobile web, Big Data, cloud computing, and the early days of the Internet of Things," the Tapscotts write in *Blockchain Revolution*. Through that lens, MIT's Brian Forde said, we can understand where blockchain fits into our lives.

"People have forgotten how powerful it is not to have to worry about what email app you use. When I email you, it doesn't matter if you're using Gmail or Outlook or Yahoo—you just give me

your email address and go. Now think about sending money today. If I want to send you $20, we're going to play a game of 20 questions. Do you have PayPal? How about Venmo?" said Forde.

"Imagine if we still chose our cell phone carriers and ISPs based on whether your friends and family were using Sprint or AT&T," Forde went on. "That's still the world we live in today for most digital services. You joined Facebook because your friends did. You're not going to sign up with a new payments startup if your friends are all on PayPal. It's going to be incredibly powerful for consumers to have more choice when everything running on blockchain just *works*."

## 10 Blockchain Startups to Watch

Tons of innovative startups are pushing the envelope of what's possible with blockchain technology. Here are other 10 exciting companies to keep an eye on as the space evolves:

**Abra:** A blockchain-based digital wallet that lives on your smartphone. Abra allows you to send or receive funds from any source in the world, without requiring bank accounts or transfer fees, using its own community of "tellers."

**Augur:** Through Augur's decentralized prediction market, you can bet on events in the real world. Using blockchain-based tokens, you can make wagers on pretty much anything, from the score of a game or winning lottery numbers to whether or not an Antarctic ice shelf will collapse (that's a real betting market on the site).

**BlockCypher:** This company is a cloud-based Web services platform for blockchain apps. What Amazon Web Services (AWS) is to cloud infrastructure, BlockCypher wants to be for blockchain.

**Bluzelle:** Between Bitcoin, Ethereum, and all the other blockchains out there, the industry already has interoperability issues. Bluzelle is middleware that supports all blockchain protocols and smooths out banking and payments transactions in what CEO Pavel Bains describes as the "Red Hat of blockchain."

**Brave:** Founded by Mozilla co-founder Brendan Eich, Brave is a new kind of browser that automatically blocks ads and trackers and instead helps drive publisher revenue through blockchain-based micropayments. As ad revenues for the digital media industry continue to decline, Brave's micropayments model could be an answer.

**Credit Dream:** Access to credit can be difficult to come by in developing nations, and carry enormous interest if you're lucky enough to get it. Currently active in Brazil, Credit Dream is a mobile-based blockchain platform for connecting investors in any country to loan borrowers in any country for affordable, verified loans.

**Enigma:** A stealth startup from MIT Media Lab, Enigma takes the blockchain's privacy and security advantages and rolls them into a decentralized cloud platform that guarantees privacy. Enigma encrypts and protects data even when you share it with others, allowing data to be stored, shared, and analyzed without ever being fully revealed to any party.

**Slock.it:** Slock.it is the manifestation of how blockchain and the IoT fit together. Built on the Ethereum blockchain, the startup is embedding smart contracts in connected cars, homes, and other IoT devices with the goal of enabling anyone to rent, sell, or share their connected property without a middleman. Think about renting your apartment on Airbnb with Slock.it automatically opening and locking your door.

**Plex:** Plex uses the Ethereum blockchain, machine learning, and artificial intelligence to give insurance companies real-time remote diagnostics on cars and drivers.

**Zcash:** As cryptocurrencies go, Zcash is the most exciting one this side of Bitcoin. Zcash uses something called zero-knowledge proofs to create truly anonymous digital transactions. While it's mined on a public blockchain just like Bitcoin, Zcash provides a fully anonymous cryptographic key in which no private information needs to be exchanged. Next to Bitcoin, it currently has the highest price of any cryptocurrency.

Blockchain is taking root within a wide swath of industries. To discover which ones, all you need to do is follow the money. A Deloitte survey released in December 2016 polled blockchain-knowledgeable senior executives at organizations with $500 million or more in annual revenue. Of the 308 respondents, 28 percent reported that their companies have already invested $5 million or more in blockchain technology, with 10 percent investing $10 million or more. Although the fintech industry was early to show interest in blockchain and accounts for a significant amount of investment and activity, the survey revealed other industries aggressively pursuing blockchain.

Within the consumer products and manufacturing industry, 42 percent of respondents said they're planning to invest $5 million or more in 2017, compared to 27 percent in the media and telecoms industry, and 23 percent in financial services. Put together, 30 percent of consumer manufacturing and media/telco industry respondents said their companies have already deployed blockchain into production.

Yet the industry the Deloitte report identifies with the most aggressive deployment plans is healthcare and life sciences: 35 percent of respondents in that industry say their companies plan to deploy blockchain in production within the next calendar year. When you look at some of the blockchain healthcare initiatives already out there, that stat starts to make a lot of sense.

One exciting project Forde pointed to is MedRec, an MIT initiative creating a blockchain to serve as a digital family history of medical records.Think about sitting down in a doctor's office and being asked your family medical history for a certain illness. You might, off the top of your head, have no idea of the answer. But with MedRec blockchain, families and medical providers can create a shared medical history that can be passed from generation to generation.

"With medical records, we're all asked that question: Is there any family history of this? The answer is usually 'I don't know,'" said Forde. "What's interesting here, as a result of the Affordable Care Act (ACA), we now have this mandate for electronic health records, and the government subsidizes doctors to get those records. But that data is still siloed. There needs to be a technology or protocol allowing all that data to be shared, regardless of provider. MedRec helps facilitate that. It's not just about the interoperability of your data; it's also about the protection of your data from fraud."

Forde said the project is also evolving as a way for hospitals and medical practices to interface with consumer tech. Think about all the real-time health data collected by wearables and fitness trackers and even apps like Apple Health. MedRec is exploring the possibility of using blockchain to give doctors and hospitals access to that data, if you consent.

"You've got Fitbit, Apple Watch, all this consumer tech collecting data on your blood pressure, heart rate, etc," said Forde. "Then you go to the hospital or your doctor and they have their own system. You see the allergist and they've got their own system, and none of it is connected. If there's no interoperability between any of these systems, how are you going to get the best possible care?"

The federal government recognizes blockchain's potential for health care, and the Department of Health and Human Services (HHS) is already doing something about it. The HHS Blockchain Challenge gathered more than 70 submissions of academic papers on blockchain usage in health IT and health-related research, announcing 15 winners this past September spanning organizations including Deloitte, IBM, MIT (MedRec was one of the winners), and The Mayo Clinic. The winners, who presented to the HHS for possible development and implementation, proposed blockchain solutions for everything from health insurance claims and payments to data interoperability and Medicaid applications. The Chamber of Digital Commerce, which participated in the challenge, sees blockchain's potential to transform healthcare and beyond.

"HHS received so many amazing ideas," said the Chamber's Boring. "In the healthcare industry, we are seeing a huge influx of interest and a lot of major problems blockchain is addressing, from patient privacy and electronic health records to tracking pharmaceuticals and doctor shopping. Blockchain technology is also extremely powerful when it comes to victims of identity theft.

Blockchain provides for an unprecedented level of privacy and security that can be leveraged to confirm your digital identity as we do more and more of our daily activities online."

That notion of identity is key. Through the digital "wallet" a blockchain creates around not only virtual money but the pieces of data that make up your identity, blockchain will act as a gatekeeper of sorts to how we interact with the digital world. Blockchain-based identity is being explored and experimented with in a host of ways, from the IoT governance model to more secure voting, and in the case of Blocksafe, as a way to reduce gun violence by securing firearms with "smart locks."

"These digital wallets will become control centers," explained Bloq's Garzik." In a multi-chain, multi-network world, you wind up with a digital experience that secures itself with several factors of authentication.Then once [the blockchain verifies] that I'm Jeff, it'll say things like, 'Do you want to send your autonomous car from home over to your wife's office? Do you want to unlock the door for a guest coming over? Are you allowed to drink at this bar? Are you licensed to carry a gun?'"

One of the futures envisioned in *Blockchain Revolution* is a "second era of democracy": one in which blockchain technology can create the conditions for fair, secure, and convenient digital voting that galvanizes the citizenry by removing so many of the systemic voting roadblocks plaguing our current system. Putting democracy on a blockchain is complicated, but startups including Follow My Vote and Settlemint are already laying out frameworks centered around blockchain-based tokens serving as votes, dropped in digital wallets for each candidate.

At a time in America when the integrity of our voting process is under intense scrutiny, blockchain—as with every manifestation of the technology laid out in this feature—could provide a new way forward. The book points to a 2015 paper published by the University of Athens introducing DEMOS, an end-to-end e-voting system, and an organization and "political app" in Australia called Flux that's already using blockchain voting to try to transform the political process. When I spoke to Don Tapscott for this story, he discussed how the opportunity to "reinvent democracy" speaks to the universal power of what blockchain can do.

"Young people didn't vote in [the 2016 presidential] election because they're not engaged. We urgently need to fix this. In the book, we argue for a new era of democracy based on accountability, smart contracts, and a culture of public deliberation and active citizenship enabled by the blockchain," said Tapscott. "We should move many things onto blockchains. I think governments could move toward creating a blockchain-based identity. Think about your health records, your academic records, your citizenship and ability to vote, all unified and facilitated via blockchain. As a voter, you need 100 percent assurance that your vote was counted for the person whom you voted, that it can't be reallocated, and that it was private. In e-voting, only blockchains can guarantee that level of assurance.

"But it goes far beyond e-voting," Tapscott continued. "Leaders could come to power with a smart contract where they're accountable to citizens and have to abide by the terms of the contract. There are opportunities everywhere. Look at the different hats we all wear every day. You're a parent, a consumer, a listener of music, an employee, a voter, a citizen. Blockchain affects you in every way."

Reference: https://www.pcmag.com/news/blockchain-the-invisible-technology-thats-changing-the-world