HEALTH WEALTH CAREER

BLOCKCHAIN

EVERYTHING YOU NEED TO KNOW ABOUT HOW THIS REMARKABLE TECHNOLOGY WILL IMPACT YOU, YOUR ORGANIZATION AND SOCIETY

PETER FUCHS

CONTENTS

INTRODUCTION 1

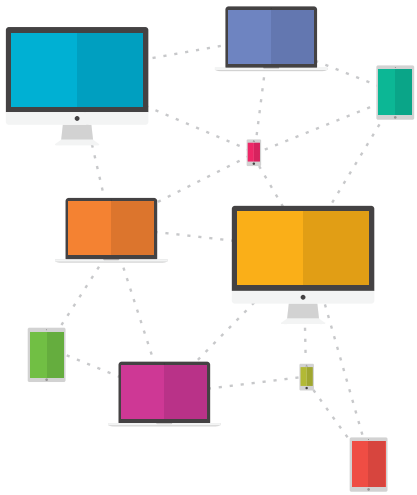
BLOCKCHAIN BASICS 3

THE IMPLICATIONS OF BLOCKCHAIN 10

REALITY CHECK 20

CONCLUSION 22

INTRODUCTION



In recent years, "blockchain" technology has been gaining more attention from the mainstream press. Heralded by some as the fourth wave of computer technology with implications potentially as profound as the advent of modern property rights, blockchain represents far more than the Bitcoin cryptocurrency with which it is often confused. In its simplest form, blockchain is nothing more than a new type of data structure. But by bringing together a number of existing technologies in a novel way, blockchain technology secures the integrity of a network — essentially codifying "truth" and eliminating the need for "trust." The implications are vast, and perhaps most important is the ability to exchange anything between two parties without the need for an intermediary. The asset can take any form — even intangible things like sensitive information — and the parties involved may not even be known to each other. Blockchain enables a nearly frictionless exchange of value, much like the internet has enabled a nearly frictionless exchange of information.

In spite of all its potential, blockchain is not a silver bullet. While the pace of global technological change is accelerating, the adoption of blockchain technology will take time and likely will follow a trajectory similar to the internet around the mid-1990s; some benefits will be realized in the short term, but it will take decades for blockchain's full potential to be reached. As we'll explain, blockchain's value is highly dependent on broad adoption, so widespread transformations won't be visible to most people until a tipping point has been reached.

This paper introduces blockchain technology and explains how its unique characteristics could help fundamentally change the building blocks of commerce and society. Perhaps unfortunately, a certain level of familiarity with the technical elements is necessary to appreciate its potential, so Part One provides a summary of what blockchain is and how it works, using as few details as possible. Part Two explains how blockchain is being used today, how it may be used in the near and long term, and why it is important to people and organizations far from the front lines of technology. While blockchain technology holds a lot of promise and can generate powerful economic forces, it does have its limits and some entities will deliberately strive to slow its adoption. Part Three explains what's behind some of this.

It's important to note that many of the developments described won't be applicable until several years from now, perhaps even decades. We're not suggesting that everything will happen precisely as we lay it out — only that the technology now exists to make it possible. As such, it is not a call to action but, instead, a call to awareness. In some areas, you may end up with more questions about blockchain than you had when you started, but with a basic understanding we hope you will be in a better position to consider how this technology may have an impact on the social, commercial and societal elements most important to you and your organization.

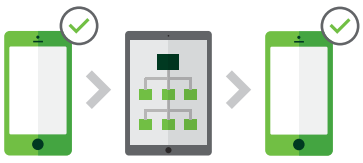
BLOCKCHAIN IN THREE BULLETS

Whether this is your first article or you've read dozens and you're trying to come up with a simple way to explain blockchain to others, three key ideas summarize what the technology does and why it's important. It can get much more complicated, but if you believe it's possible to acknowledge that the internet is a powerful technology yet not really understand how it works, then you can do the same for blockchain. Forget terms like consensus, disintermediation, distributed ledger, mining, ICOs, hashing and private keys. Just remember these three points.

WITH BLOCKCHAIN:

- **Data can act just like a physical object.** Through a physical process called "tokenization," blockchain makes it possible for a data "asset" to exist in the digital world just like a physical object does in the real world. Virtual and real become indistinguishable.

- **There can be a single version of truth that everyone can agree on.** When using blockchain technology, once information is captured accurately it never needs to be verified. Operational processes can focus on first-time accuracy instead of ongoing validity, and there is never a need to reconcile anything.

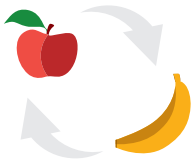


- **Intermediaries are not needed.** All exchanges of information happen as intended. Blockchain creates an (almost) absolutely reliable method for transmitting information. Party A (who really is Party A) sends item X to Party B, who gets exactly what was expected, every time. With the exchange process inherently and verifiably valid, nobody needs to vouch for anything.

If that's enough for now, then feel free to skip to Part Two. But if you'd like to know a bit more about how blockchain works read on.

PART ONE

BLOCKCHAIN BASICS



UNDERSTANDING INTEGRITY AND TRUST

To understand the value of blockchain it's helpful to first consider the basic concept of value exchange. If we go back to the early days, people traded goods in person through barter. Both parties were able to see and verify what they would be receiving — your banana for my apple.The certainty, or integrity, of the process was validated by the ability to see and touch the goods to be traded.

But as people sought to exchange larger quantities of goods over longer distances, things got more complicated. Merchants couldn't necessarily trust that the expected goods would arrive as promised, nor was it practical to personally inspect the entire contents of a wagon or ship before a trade could happen. It was no longer possible for parties to ensure the integrity of a transaction.

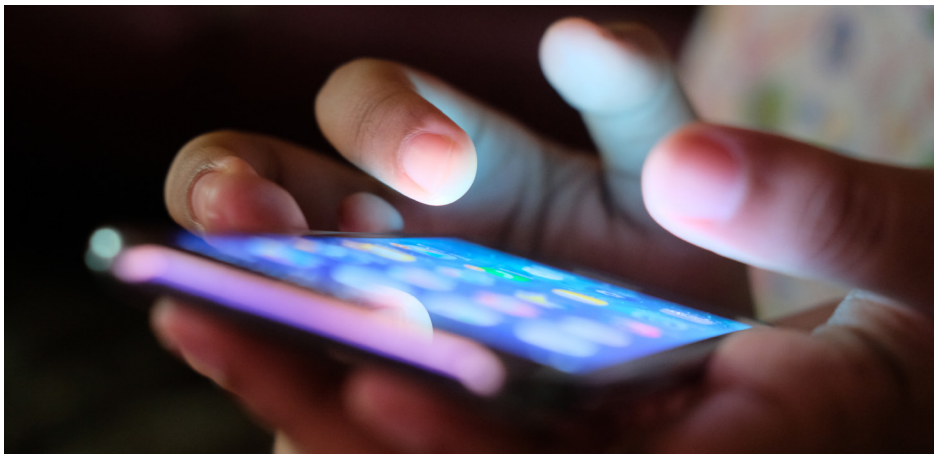
So intermediaries emerged to play that role. They built reputations as trusted agents who, for a fee, would vouch for a transaction on behalf of the trading parties. This was true not only for commercial transactions, but also for the communication of all kinds of sensitive information. Trust became the stand-in for the shortcomings and vulnerabilities of the process.

Blockchain makes it technically possible to ensure the integrity of information and the process of exchanging it.

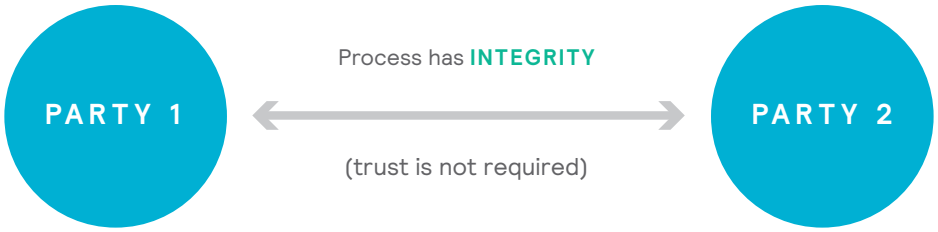
Many different methods were attempted to improve the integrity of the process, to ensure all the parties to a transaction or exchange got what they expected. But for most of history, technology simply hasn't been available to do that. Documents could be altered, communications could be intercepted and signatures could be forged.

The internet has changed things dramatically over the last few decades, and now it's relatively easy to reliably exchange information over long distances among unfamiliar or untrusting parties. But many challenges remain, and organizations invest a tremendous amount of resources in cyber threat prevention, detection, mitigation and recovery, and in many settings computers and the internet have simply replaced paper-based processes with electronic ones.

For the first time in history, blockchain makes it technically possible to ensure the integrity of information and the process of exchanging it.



Fom this perspective, it becomes easier to see why blockchain is potentially so valuable — and so disruptive. With integrity assured, trust is no longer required and the need for an intermediary to validate what is "true" has been eliminated. Rather than simply digitizing old ways of connecting parties who wish to exchange information or value, blockchain makes it possible to fundamentally redefine the building blocks that determine how value is stored and transferred.



BLOCKCHAIN BUILDING BLOCKS

Blockchain is a term that actually describes a collection of complementary technologies. Although each of these elements has existed in some form for many years, blockchain brings them together in a way that can result in significant benefits to network integrity, information security and connectivity. The building blocks vary, but they most commonly include:

AUTHENTICATION

Methods to prove that you are who you say you are

ENCRYPTION

Methods designed to limit access to data by making it unreadable unless identity is authenticated and permissions are verified

DIGITAL SIGNATURES

A digital stamp to establish proof that someone did something

HASHING

An algorithm that converts a data file into a unique string of characters (think of it as a “digital fingerprint”) and see page 6 for a more detailed summary

HASH FUNCTIONS

HASHES SERVE AS A BRIDGE BETWEEN SECURE AND UNTRUSTED ENVIRONMENTS

To the non-technical, the whole subject might seem like a deep-dive that should be reserved for coders and security gurus. But, in fact, hashing plays a really important role in most blockchain applications and serves as a bridge between secure and untrusted environments, so it's actually really important to understand its basic principles. There are a wide variety of hashing methods, but the basic purpose to is transform data files of any length into a unique string of characters of the same fixed length. This makes it very useful for comparing files without revealing their contents.

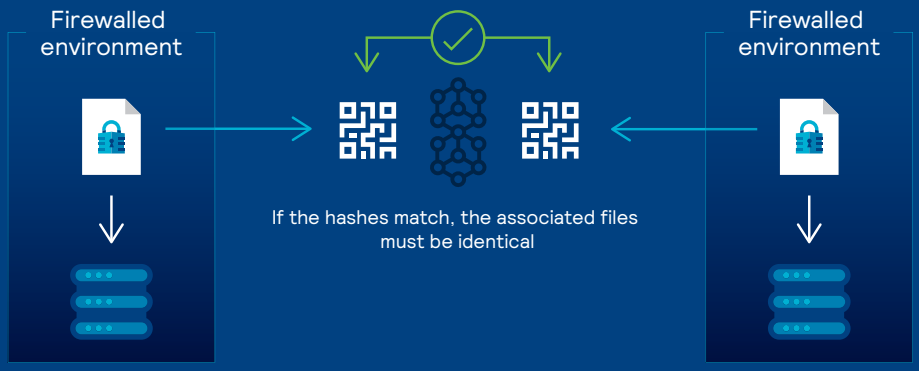
One way: The INPUT cannot be derived from the OUTPUT.

Repeatable: A given data input will always have exactly the same output each time it is run through a hash function. It's not random.

Unique: If just one bit of data in the input file is changed, the resulting hash output will be completely different.

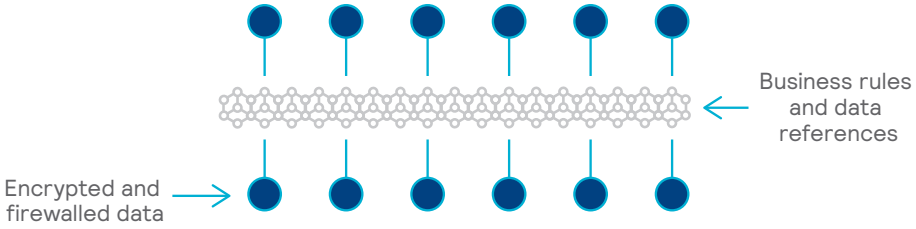
The original data file can be a book, a song, an image, a movie, a computer program's source code, a patient health record, a highly confidential commercial contract, secret government intelligence data … anything. Just like a human fingerprint, hashes provide powerful security possibilities because they can be compared openly to verify that the different versions of confidential data they represent are identical.

Unlike encryption, which is a bidirectional transformation process in which data can be encrypted and decrypted, hashing is a unidirectional. A data file is fed into a hashing function, and what emerges is a string of characters that cannot be "reversed" to derive the original data. It would not be possible to discern the original data, but it is possible to determine whether two hashes are the same and therefore represent the same primary data file — just like a human fingerprint.



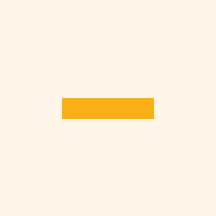
THE BLOCKCHAIN NETWORK

Before explaining how a blockchain is built, it's important to understand exactly what makes up the network. Participating computers are called "nodes," which are simply computers that can store the blockchain's data, follow the rules of the blockchain's specific protocol and communicate with the other nodes. Nodes can be physically located anywhere, and for this reason they're called "distributed." Each node follows the same rules and maintains an identical copy of the blockchain data set.



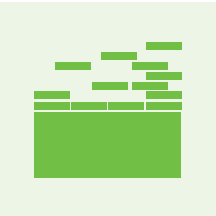
BUILDING A BLOCKCHAIN

A number of blockchain protocols exist, but they all pretty much do the same thing and each has four basic elements: the transaction, block, chain and consensus process.



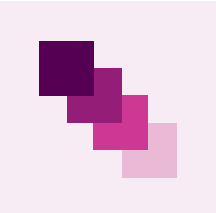
THE TRANSACTION

The most basic component of a blockchain is a transaction. It may represent an exchange of something valuable (literally, a "transaction") or it may be a hash file representing something as simple as a single word or as complex as a software program. Whatever it is, the submitting party digitally signs it, and when it's received by the network, it's time-stamped.



THE BLOCK

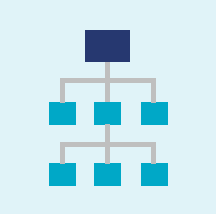
The transaction is then added to a "block" that includes other new transactions. The size of the block and how fast it gets filled up depends on a number of factors, including the particular blockchain protocol.



THE CHAIN

When the new block is full, it is linked to the preceding one through a clever hashing process that makes blocks more and more secure the longer they've been a part of the chain. Once the new block is added to the chain, it is not possible to change any of the preceding data. This makes the data immutable. Because transactions and blocks are assembled in the order they're received, as the blockchain builds it forms a chronological record of activity. Much like a record in accounting, it forms a ledger.

CONSENSUS METHODS:
The more common methods of establishing consensus include "proof of work," which involves a puzzle-solving process called "mining," and "proof of stake," in which the new block to be added is selected from among network participants according to a variety of criteria. A number of factors will influence which consensus process should be used for a particular blockchain, including whether it's intended to be widely accessible and the rate at which new data need to be added. Note that "valid" and "truth" in the consensus context are synonymous, but neither necessarily means "correct." In other words, it is possible to write "false" information to a blockchain. Just like any business or administrative process, the rules governing the content must be designed to identify incorrect information.

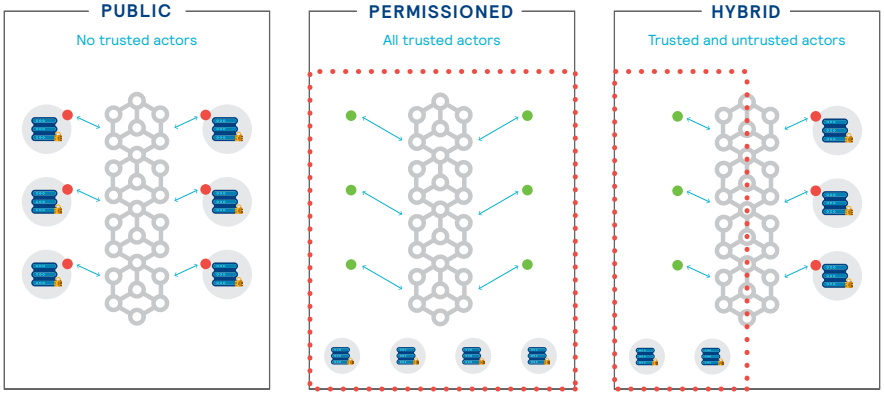


THE CONSENSUS PROCESS

Before a new block is permanently added, the network participants complete a process to confirm that the newly updated version of blockchain, including the new block, is valid. This consensus process can take a number of forms, but the goal is for each of the network participants to agree that the block has been assembled and added according to the rules of the network. This is a critical feature of the blockchain concept, because it is this consensus that establishes a single record of "truth" that all participants will agree with. When consensus is reached, the newly updated blockchain is then replicated among all of the participating nodes in the network. Because they have all agreed in advance on the rules establishing how the database will be managed and each has an identical copy, any attempt to change the data in one version would be easily identifiable by any of the other network participants.

TYPES OF BLOCKCHAIN NETWORKS

Blockchains can be public, private or a hybrid, and the overall purpose of a blockchain will determine which is best. But the real value of blockchain technology is realized only when the widest possible number of users are able to access data, so if all participants in a network are truly "trusted," then blockchain may not be the best technology option. It's likely that public blockchains will play an important role as the technology develops. For that to happen, technical and non-technical people will have to get comfortable with hashes and other references derived from their confidential data being placed on public blockchains. That will likely be no small task, and will take quite some time.

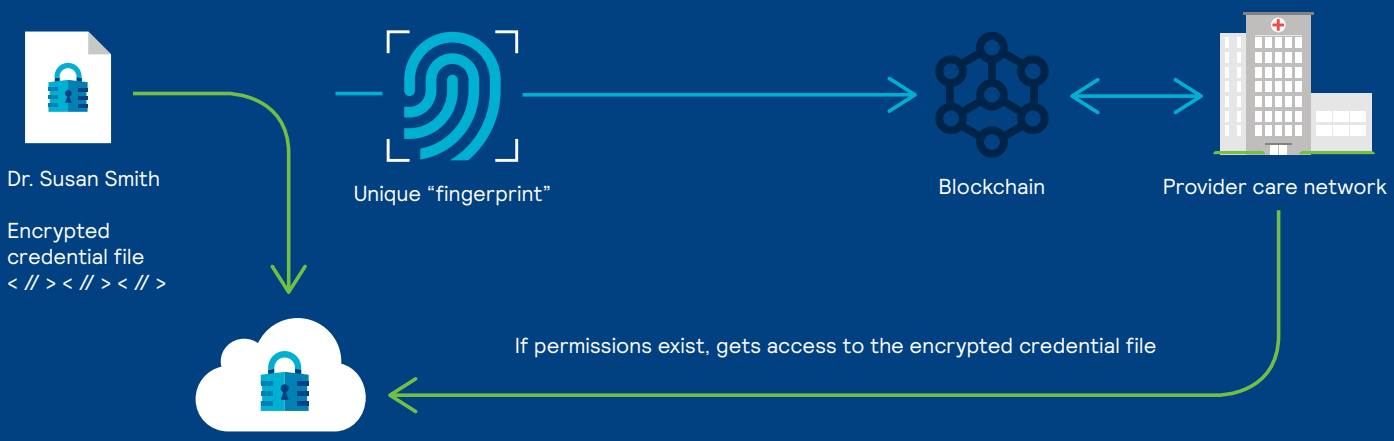


So transactions are assembled into blocks, new blocks are connected to preceding ones, and the entire chain is replicated on each network node. As each new block is added, all nodes must agree. The result is a chronological, immutable ledger. It is a single source of truth where trust is not required, and those that had once served to validate the process played no part.

"ON CHAIN" VS. "OFF CHAIN": WHERE THE DATA ACTUALLY LIVE

It's important to note that while anything is possible, primary data are not usually stored on a blockchain. Instead, only a representation of the data, sometimes a hash of the file, is written "on chain," along with some associated metadata that provide identifying information and references to the "off chain" location of the primary data. It's better to think of a blockchain as a method that creates a reference table to connect data, not collect data.

Example: Instead of storing a document that includes the details of a specific doctor's education and licensing credentials a blockchain, a reference file is written "on chain" and the supporting documents are stored in a secure database off-chain.



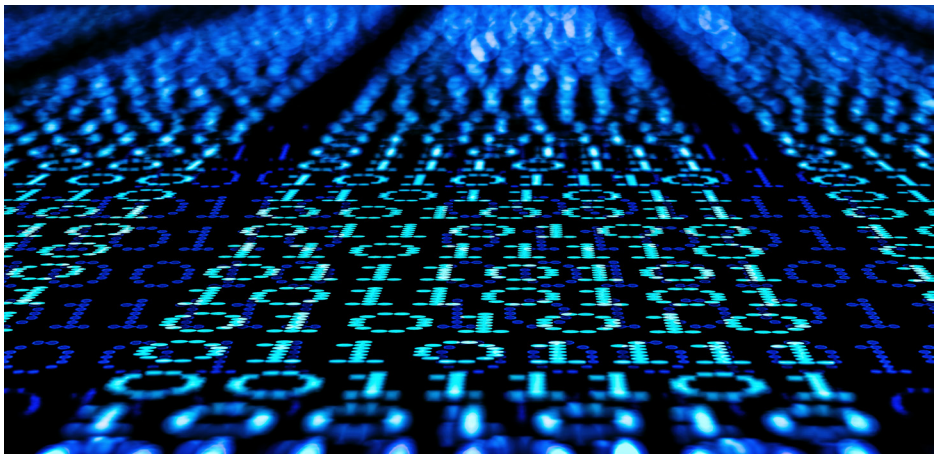
An analog example might be a library's paper-based card catalogue, where a volume's reference card would include important information about a book, such as the author's name, date of publication, a description of the contents and the location in the library where the file can be found. In this analogy, the card catalogue represents the blockchain, and the library represents the internet. It includes all of the associated shelf space containing the important information, and may even include other library locations, much like the internet includes many separate databases.

PART TWO

THE IMPLICATIONS OF BLOCKCHAIN

REINVENTING HOW DATA ARE CONNECTED

Blockchains have the potential to change the basic framework of information storage and exchange by simplifying how computer networks connect and how data are linked to a common subject.



Blockchains can significantly reduce the complexity of computer networks.

Reducing Complexity

Blockchains can significantly reduce the complexity of computer networks. Today, each new participant has to be linked to the existing ones through an independent connection. Application programming interfaces (also known as APIs) are a good example. As the network grows, its complexity increases exponentially. The larger it gets, the harder it is to grow further.

With a blockchain foundation, new nodes simply join the network and can automatically have access to the same reference information. Complexity increases linearly, making the network far easier to scale.

Increasing Connectivity

To get the most complete picture of a subject, it's necessary to find a common element and organize information around it. For example, a common data subject is an individual person, and organizations of all types spend vast amounts of resources in an effort to connect information about each of us. This process, called data attribution, provides the foundation of analytics, which requires related data to establish correlations and make predictions.

Linked by blockchain references, vast amounts of data about a subject can be tied together and yet simultaneously remain independent, anonymous and secure. As a result, downstream automated processes like artificial intelligence (AI) and machine learning can use larger volumes of higher-quality data, improving the output of existing analytics while also enabling techniques that weren't previously possible.

ASSET REGISTRY EXAMPLE

A new house is to be built in a small town in the United States.

- The deed for a parcel of land has been recorded on a blockchain by the town clerk.
- The land is purchased by a builder, who is issued permits that allow a single-family home to be built.
- Inspections are completed by town officials at various points in the construction, and when the house is complete the local government does a final check before issuing a certificate of occupancy.
- The deed for the land is updated to reflect the new house.
- The builder then lists the property for sale.
- Eventually an offer to purchase is accepted, and the town clerk records the transfer of the deed from the builder to the new owner.

Each of these steps is recorded on a blockchain, and all other interested parties can view the details, confident that they occurred as reflected on the record. The record is permanent and all subsequent changes are captured for future parties.

Through these two features, blockchain is making it easier to perform powerful analyses that improve everything from our commute to our healthcare, or even just to make our lives a little easier.

SO WHAT IS BLOCKCHAIN GOOD FOR?

Blockchain is well suited for a number of applications, It's vital to remember that blockchain is most useful when information or other assets need to be exchanged among a number of parties who may be unfamiliar or untrusted.

That "sharing" part is important, because if data will be used only within the bounds of an organization's own computer network, then existing technologies and security protocols are likely good enough. But if data will be shared across security borders, then blockchain is well suited for several common functions in the process.

Asset Registries

An asset registry is simply a list of who has what. For example, government agencies issue deeds and titles to confirm ownership in real property, which may include land, cars and other equipment, and intangible assets like patents, trademarks and other intellectual property. Each of these is an asset registry. Other examples would be a rental car company that keeps a list of all the vehicles it owns, or an art gallery that tracks all the pieces in its collection.

Each of the building blocks explained earlier, including authentication, encryption and digital signatures, plays an important role in establishing a permanent recordkeeping system, and blockchain's chronological feature provides a historical record of activity — not just the current state.

The registration of data on a blockchain can actually serve to "create" an asset. This is called "tokenization." Tokens can become a very efficient way to manage information or assets. Because blockchain makes it possible to have just one copy of data, supply and demand dynamics can develop. A digital file, such as an image, a song, a movie or even a cyberpet, can be made "rare," and value will adjust with demand. That's essentially how cryptocurrencies work; each "coin" is a nothing more than a digital file with a value that is often assigned entirely through demand sentiment.

Reconciliation and Audit

As data are recorded to the network, they are immediately replicated among the participating nodes. Because each node has an identical copy, and all the nodes agreed on the process by which the data would be recorded, there's no need to reconcile one party's version of the truth against another's version. Similarly, the chronological and immutable record makes audit automatic, because the blockchain provides both proof that a sequence of events was followed and the state of data at each point in time. The permanent, immutable nature of the recorded data also makes it a powerful tool in fraud prevention.

This has significant implications on the accounting function, since the rules by which transactions must be recorded are well established and can (theoretically) be codified into the blockchain. In the future, the monthly, quarterly and annual reporting process will largely be automated, and financial statements will be able to be generated and audited in real time. Human judgement will still be required in unusual situations, but accountants will be freed from much of the tedious recordkeeping and audit testing that defines much of their work today. They'll be able to manage the exceptions rather than the routine, and when provided with access, regulators will be able to tap into a single source of an organization's validated data at whatever detail the law permits.

Transactional Processes

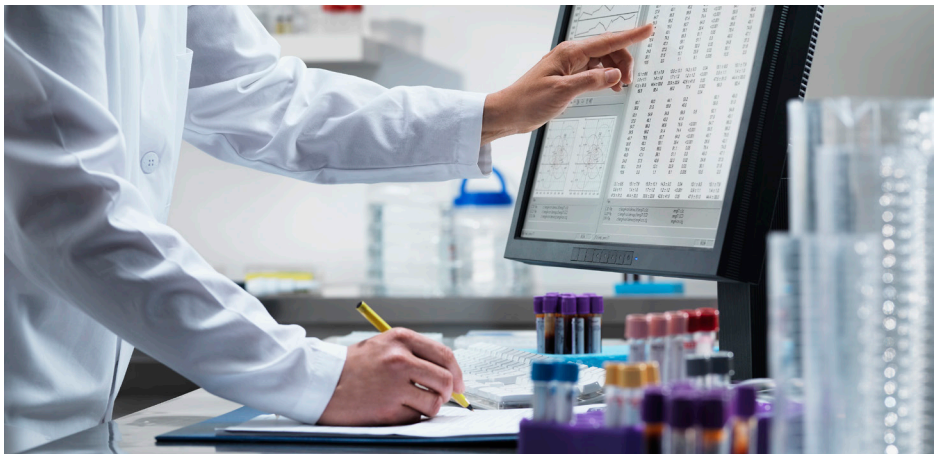
Where large volumes of data are collected, the blockchain is a very effective method to initially capture the information and to serve as a platform for further analysis. On some blockchain protocols, computer programs called smart contracts can even be written at the database layer to automate contractual terms and execute when certain events occur. Insurance claim management is a good example.

While this may seem similar to existing technologies, it's actually very different. Because the programs are written to the blockchain and shared among all the participants in the network, the programs in each node are identical. Because the inputs are identical and the programs to process them are identical, the outputs must be identical. It's as if each network participant is running the same process independently (which is actually happening), but all the participants are doing it simultaneously using the same network and sharing the result immediately.

Note that some current blockchain protocols are not capable of handling extremely high-speed, high-volume processes. For example, thousands of credit card transactions are processed per second, and the consensus process necessary to validate a new block in proof of work protocols is generally limited to a new block every few seconds — or even every few minutes.

WHERE IS BLOCKCHAIN BEING USED TODAY?

As seen in the early days of the internet, most of the current blockchain implementations are focused on improving back-office efficiencies and reducing the time and cost of operating processes. As these administrative processes mature, they will provide the foundation for new customer-facing commercial and strategic opportunities. A quick online search will provide many examples of how blockchain is being used today, but a few examples include:



Most banking institutions are adopting blockchain and advanced distributed ledger technologies for a wide range of functions.

Financial Services

Blockchain technology was originally devised as the foundation of Bitcoin, the first digital currency. But experts were quick to realize that the technology represented far more, and that it could eventually change financial services as profoundly as the internet had changed media and entertainment in the 1990s and early 2000s. Most banking institutions are adopting blockchain and advanced distributed ledger technologies for a wide range of functions, including trade settlements, payment processing and cross-border transactions.

Healthcare

The global healthcare industry manages vast amounts of clinical and administrative data, from the pharmaceutical supply chain to patient medical records and claims management. The introduction of smart medical devices — including everything from personal fitness trackers to connected surgical suites — presents an entirely new ecosystem of information to mine, and the pool of data collected is growing exponentially. Accurate, accessible data are critical to improving clinical outcomes and reducing waste, and blockchain's immutability and ability to connect currently siloed information and serve as the "single source of truth" are key enablers.

Government

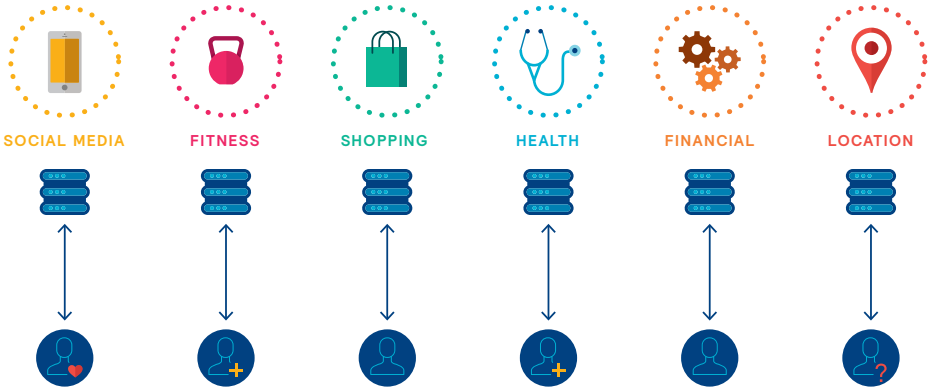
Governments around the world, including those in Denmark, Dubai, Estonia, the European Union, Georgia, the Isle of Man, Switzerland and the United States, are already using blockchain for everything from property records to voting. Its ability to provide a chronological, immutable, single source of truth makes it ideal for individual identities, property records, patents and other primary data.

CAPTURING OUR "DIGITAL EXHAUST": BLOCKCHAIN ON AN INDIVIDUAL LEVEL

Our lives are filled with devices that create and capture data about us. From the smartphones in our pocket to the dozens of Internet of Things devices we're adding to everything from our automobiles to our toasters, we're streaming data at an ever-increasing rate. It's a continuous stream that for some people already includes every step, every mouse click and even every heartbeat. That information represents a sort of "digital exhaust" that is unique to every individual.

The data are already being collected, but blockchain provides a technical platform to organize, secure and connect it while the sensitive primary details remain stored in separate off-chain databases. By continuously registering representations of our streaming data onto blockchains, all of the effort and expense that public and private organizations put into connecting the dots today will eventually become automatic. These linked streams can be used to create an extremely detailed portrait of who we are and what we do, and enables powerful data analyses to inform our personal and professional lives. But who will decide how this information will be used?

Today, from social media to our fitness tracking devices, our data are fragmented among the dozens of companies with whom we each have accounts. Although the thread that is common to all of it is each of us as individuals, for the most part the information collected is considered the company's "proprietary" data. Legal data rights are beginning to migrate to protect individuals and privacy, but information remains siloed.



TODAY Individuals have multiple, independent accounts

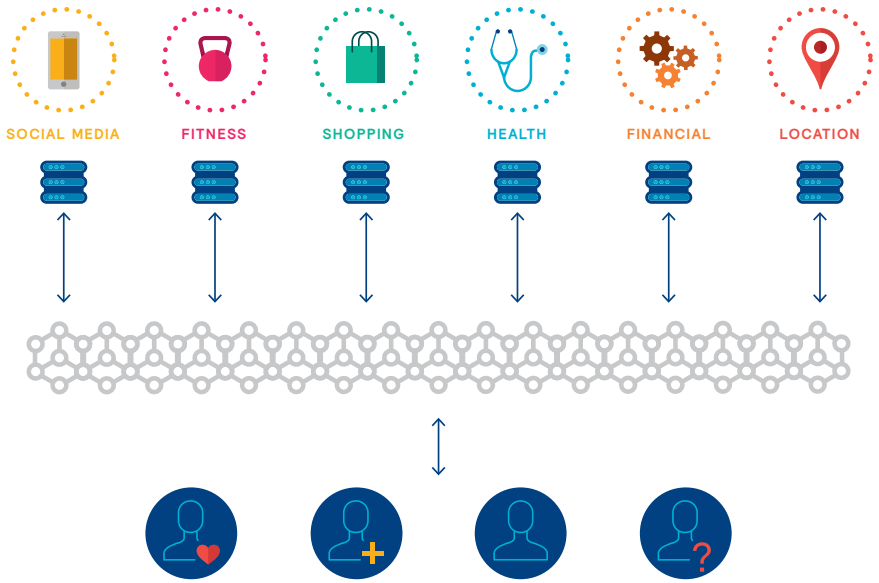
Despite the large volume of information, we have very little ability to influence how the data are used or to analyze it ourselves. In fact, the end-user license agreements we have to accept from many digital service providers typically require us to give up any rights to the data we generate. The information itself remains isolated, and for the most part we're not able to link any of the information together. From time to time, service providers announce partnerships where they've made it possible to link certain elements, such as our smartphone and our fitness tracker, but those examples are the exception.

Although an ever-increasing number of data sources collected seem to threaten the very notion of privacy, the regulatory momentum continues to favor the individual's right to control how personal data are used. And while application today is imperfect, the right to privacy is at the center of most western legal frameworks.

In the United States, HIPAA (Health Insurance Portability and Accountability Act of 1996) establishes national standards to protect individuals' medical records and other personal health information. Other regulations establish protections around a person's financial history, employment information and other data.

In the European Union, a sweeping new body of law called the General Data Privacy Regulation (GDPR) became effective in May 2018 that firmly establishes the basic legal framework surrounding the data rights that apply to all of its citizens no matter where they live. Through the GDPR, the European Union is laying the foundation for the primacy of individual rights, and included are issues of data privacy, ownership, control, giving and revoking consent, and even portability, which gives individuals the ability to use data for purposes other than for what they were originally collected. The regulations apply to any organization that interacts with an EU citizen, and they have the ability to levy considerable penalties to violators.

In the future, legal standards will mandate that individuals have more control over their data, and blockchain is among the technologies that will make that control possible.



TOMORROW

With a handful of "personas," individuals will decide how to link their data and how to share it

Driven by supply and demand and economic forces of a consumer- centric consumption economy, incentives will develop to encourage people to allow others to access their data. As early services emerge that enable the connection of a few sources, consumers will be able to monetize that data by renting access to their profiles to companies that want to sell products and services to consumers like them. Unable to control competitors' access to customer data as they once did, businesses will have to differentiate through their ability to deliver unique and relevant analytics as they develop and continually tweak their offerings. Incentives offered to these willing consumers may be in the form of free access to services that unwilling users would have to pay for, or direct monetary compensation.

It will also become possible to establish consistent, portable reputation scores that describe the scope and quality of data an individual makes available, and the even the effectiveness of earlier efforts to sell to that consumer. As more data sources are connected and deeper access permissions are given, more powerful predictions of behavior will be possible, increasing the value of the individual's profile. In effect, individuals will be able to self-identify as willing marketing targets with a comprehensive descriptive profile — a development that will radically alter the business of advertising as we know it.

HOW BLOCKCHAIN WILL IMPACT SOCIETY AND ORGANIZATIONS

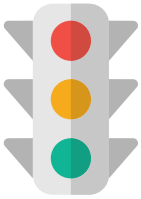
Blockchain makes it technically possible to create a person-centric society where data is consistently, reliably and securely organized around each individual.

Direct-to-consumer advertising is only one example of blockchain's impact. The same type of analytics that drive the consumer economy will be relevant across every facet of modern society, including basic social functions. This will eventually have a profound effect on how people relate to one another, their employers, organizations that provide the goods and services they consume, and governments.

Digital Identity

The most basic building block will be a uniform method to establish an individual's identity — the "personhood" record to which all other identity-related information can be tied. Everything from basic documentation, like passports and qualification for social services, to education, driver's licenses, professional credentialing, health records, and voter registration will be linked. A record will be immutably connected through a chronological, immutable ledger, and all the processes that we once needed to validate identity will no longer be necessary.

Blockchain makes it technically possible to create a person-centric society where data is consistently, reliably and securely organized around each individual.



Consent and Permission Management

Blockchain can also provide a technical solution to many of the consent management issues in today's headlines. We currently lack an efficient way for individuals to control access to their data at any level of detail and to establish and maintain the related permissions, but many public and private organizations are working on this challenge. The solution will almost certainly include AI, and just as the web browser was the original breakthrough that turned consumers onto the internet, a simple consent management solution is likely to emerge as one of the early "killer apps" of the blockchain era.

These growing stores of personal data have tremendous potential value that goes well beyond stolen credit card accounts and hijacked national identification numbers. As the scope of data collected increases, these massive databases are even more inviting targets for hackers.

Today, responsibility for the security of personally identifiable data lies with those who collect and maintain it, and protecting it is an enormous and endless cat-and-mouse effort that costs billions of dollars every year. If it hasn't already, this may become too heavy a burden for many organizations to bear. Faced with relentless security threats and a legal framework in which they're responsible for individuals' data assets they cannot freely control or use without explicit consent, many organizations will be happy to give up the liability. In the future,

organizations may have responsibility only for the information they have been given access to, and blockchain technology will provide the technical means to prove consent was given, how data were used and that specific processes were followed. Authorized organizations would be incentivized to maintain sensitive third-party data only for the period needed to do an analysis. The resulting compliance burden would be dramatically lighter.

THE HUMAN CAPITAL FUNCTION OF THE FUTURE

All of this promises to have a dramatic effect on how organizations attract, recruit, hire and retain their workforces. Blockchain has the ability to automate many of the administrative functions that consume much of HR's time today. Freed from this burden, these professionals will be able to focus on far more strategic activities, such as organizational design, workforce optimization and talent development.

Over the last 40 years, the Corporate Finance function has been transformed from a largely administrative department to a highly engineered, strategically vital discipline. Next to the chief executive officer, the chief financial officer has become the most importation executive at most companies. In the next 40 years, the chief HR officer will likely see a similar transformation as the lines between operations and the workforce, both technological and human, become more blurred.

Individual Identity

Today: A patchwork of physical documents and digital files defines each individual across an impossibly vast range of accounts and databases. To prove the common connection of the data, individuals must maintain an equally vast range of usernames and passwords, answer challenge questions, provide a reasonably similar signature and perform other tasks to ensure that they are the person in question and are allowed to access the stored information.

Early impacts: Secured by an increasingly sophisticated mix of biometric, behavioral and active authentication methods, commercial identity wallet software will begin to create common platforms for establishing a portable digital identity. A common, open-source protocol is likely to be the foundation on which this critical element is ultimately established.

Fully adopted: A common, portable identity protocol provides individuals with the ability to link all of their data together.

Employee Data

Today: Organizations maintain highly sensitive databases of employees' personally identifiable information. After initial onboarding, data require active and continuous updating. Data are often replicated among multiple company systems and shared directly with third parties that provide benefits and other employment-related services.

Early impacts: As identity management services emerge and are adopted for consumer uses like banking and shopping, employees will want the same ease and convenience where their personal and professional lives intersect. Single sign-on utilities will begin to leverage common blockchain networks to connect identities. Employees will be able to link work-related resources inside and outside the company's firewall, including a growing network of employee-sponsored or employer-coordinated benefits.

Fully adopted: Employers will no longer need to store copies of employees' most sensitive data within the company network. Instead, employees will grant access to off-chain primary data maintained by governments and other public and private organizations, all linked through blockchain on-chain references. Evolving regulatory frameworks will define which work-related data will be owned by employees and which will be portable for their use after the relationship with an employer ends.

Employers will no longer need to store copies of employees' most sensitive data within the company network.

Recruiting and Onboarding

Today: Recruitment is largely a manual, qualitative process often plagued with unintentional with systemic biases. Onboarding can be a weeks-long manual process of verifying identity, work eligibility, employment history, educational credentials and professional certifications, as well as conducting background checks.

Early impacts: Identity management tools will begin to provide professionals an ability to maintain their credentials in a portable form that can be shared quickly and easily. An early example is likely to involve healthcare professionals, who currently face protracted credentialing processes when transitioning from one facility to another in many countries.

Fully adopted: Anonymized longitudinal performance data from the existing workforce will be analyzed to identify the experience and backgrounds that are associated with the most successful employees and contract workers. Qualifications and search criteria will be developed through AI, and candidates will be matched from a pool of individuals who have opted to share their data with prospective employers. Onboarding employees will simply authorize temporary access to personal data in public and private databases that are already linked to their identity.

Background Checks

Today: Third-party vendors are contracted to mine a broad range of public and private data sources to confirm and validate self-reported details. Reports may mismatch individuals and provide only a snapshot of information available at the time a report was requested. Gaps are common, and results are not portable.

Early impacts: Regulated industries that require significant, recurring identity checks adopt a method to share validated data and simplify access to results. "Know Your Customer" processes for financial transactions are an example. Blockchain technology provides an immutable audit trail of data collected and makes it possible for recently completed reports to be shared.

Fully adopted: All civil and private data, from birth records to residency information, will be linked to an individual. An inquiring organization will ask an individual to permit access to a set of data that will verify information in question. Aided by AI-enhanced consent management software that will verify and coordinate the details behind the scenes, the individual will permit access under a specific set of conditions he or she chooses. The process will be instantaneous.

Compensation

Today: Compensation details for many parts of the economy are complex at best, and increasing attention to salary inequalities and systemic biases is driving legislation in some jurisdictions that prohibits employers from asking prospective employees about previous salaries. When developing an offer for a new employee, HR professionals weigh their organization's existing norms against survey data that are self-reported by individuals or other companies.

Early impacts: Employees will have the ability to link salary history to their personal identity profile on the blockchain, giving them the option to share verified data with a prospective employer. That data may be specific, or within a range, and employers will be able to quickly determine whether their budget and the candidate's expectations overlap. This will be able to be done without actually revealing the detailed data.

Fully adopted: Individuals can choose to share all or part of their prior compensation with crowdsourcing services that anonymize and aggregate high-quality data that has been automatically validated through payroll and tax records. Detailed work history, skills matching and other macro-level market data make job comparison easier across organizations, industry sectors and regions.

PART THREE

REALITY CHECK

Despite all of its promise, the reality is that blockchain technology remains in its very early stages, and that will limit broader commercial adoption in the short term. Few production-grade examples have existed long enough to convince decision-makers that blockchain is ready for mission-critical applications. Technical standards for many elements have yet to be established, though as was demonstrated when the internet evolved from the mid-1990s, it's only a matter of time until these issues are resolved. A few decades were enough to work out many of those challenges, and in many regards blockchain is just another foundational building block that will unlock more of the internet's potential.

Regulators have to gain comfort with the unique aspects of the blockchain, most particularly with its ability to transform many aspects of the financial system. Cryptocurrencies like Bitcoin were the first application and were quickly associated with drug runners and money launderers in the darkest corners of the internet. To some degree this persists, and the run-up of prices in late 2017 and the subsequent dramatic fall, as well as the questionable legality of some initial coin offerings (ICOs), haven't helped to reassure or convince skeptics. That said, blockchain has the potential to dramatically reduce fraud, which not only can reduce the cost of prosecuting criminal activity in private sector, but also can drive savings in the government procurement of healthcare, defense and other goods and services. As result, governments around the world have already begun to use blockchain.

But blockchain will not solve every data-related challenge. Unless the particular use-case can benefit from blockchain's features, and unless multiple, untrusting parties need to share the data, it's not likely an appropriate or efficient solution. This presents a bit of a "chicken and egg" problem, because investments are necessary for an organization to develop blockchain capabilities. In return for that investment, a value would need to be generated, but the value is realized only when the ecosystem has a lot of other participants. It's the broad user network that gives blockchain technology its power. Organizations may prefer to take a wait-and-see approach. But forward-thinking incumbents and new industry entrants are playing a different game by seeking ways to leverage blockchain's capabilities to fundamentally restructure the basic value chains of most industries.

Forward-thinking incumbents and new industry entrants are playing a different game to fundamentally restructure the basic value chains of most industries.

Not waiting for the current cast of characters, they're creating "minimum viable ecosystems" where only those participants that are necessary to deliver value to the customer are included. They're taking advantage of blockchain's ability to eliminate intermediaries, and in an existential game of musical chairs they're leaving only those chairs that are absolutely necessary in the redefined structure of the industry. Catching up will be difficult, and those companies not paying attention may find themselves without a seat when the music stops.

But overinvestment and early adoption of blockchain also come with risks. Some of the biggest organizations in financial services, insurance and other industries have recognized the potential of the technology and have announced pilot projects designed to leverage it in their business processes. Although some of those efforts have been successful and led to production-grade implementations, most have not. Why?

Experimentation is a critical part of an organization's early blockchain efforts, and experts will often recommend a scientific approach involving theory, experimental design, test and analysis through proof-of-concept to identify and prove an appropriate use case. Think of it as "new business model R&D." Organizations have to not only be willing to invest and experiment, but also learn quickly to invest wisely with an eye to the future — when adoption will be wide and new industry paradigms will have been established. Because blockchain has both technological complexity and broad strategic implications, it is particularly difficult for both business and IT experts to grasp. Technologists often lean on existing methods to solve some of the problems blockchain is well suited for, but they fail to consider a future ecosystem in which data are shared among untrusting parties. At the same time, without a solid understanding of blockchain's technical details, the future state is also difficult for business leaders to imagine. There's no common ground to get the discussion started.

Organizations have to not only be willing to invest and experiment, but also learn quickly to invest wisely with an eye to the future.

Anticipating the future is difficult, particularly in environments where everyone has different motivations and conflicting priorities. When organizations begin their blockchain experimentation, early projects are often selected through a lens of the existing environment and thus may not be appropriate. It may be easier to identify those that are inappropriate for technical reasons, whereas it is harder to identify projects that are inappropriate due to business or strategic reasons.

For example, incumbent organizations that currently enjoy a dominant role as an intermediary may try to "force fit" blockchain technology into a current process in an effort to preserve an existing competitive advantage. But paradoxically, blockchain's disintermediating power is precisely the reason that other industry actors would be reluctant to join the effort. Those that see an opportunity to bypass an incumbent are likely to decline to participate or withdraw from existing collaborations.

But perhaps the most significant factor that will slow the adoption of blockchain across some commercial segments is the influence of powerful incumbents whose businesses will ultimately face wholesale disintermediation. Presented with an existential threat, they will do whatever they can to maintain the status quo. They will lobby against regulatory change, defer participation in developing blockchain networks and dismiss the viability or even the legitimacy of the technology. But history usually demonstrates that where value is created, technology eventually wins.

CONCLUSION

Mercer is the largest human resources consulting firm in the world, with more than 22,000 colleagues committed to helping our clients advance the health, wealth and careers of their most vital asset — their people. Clients seeks us out for everything from salary data to organizational design and strategies to establish benefits programs that keep employees healthy and engaged. Ultimately, all of the work we do is about individuals — the employees that our clients have — so we care deeply about things that affect them. When it becomes technically possible to connect all of the information about a person, from birth until the present, this will change every facet of an organization — including who is hired, what employees do and how companies organize, attract, compensate, motivate and retain people. This will impact everything from career development to organizational strategies. As technology advances, we offer the following takeaways to consider:

Blockchain Is Just One Piece of the Emerging Technology Revolution

The reality is that blockchain is just one of a number of evolving technologies that will support what others have called the Fourth Industrial Revolution. But unlike AI, the Internet of Things and other more visible digital technologies, it is largely an invisible enabler.

It's a Question of When, Not if

Some capabilities enabled by blockchain are already being adopted, whereas others will take decades. But if history is any guide, it is a question of when, not if, the benefits are simply too powerful.

Like any network technology, the slowest critical network participant will establish the pace of adoption. The adoption rate will depend on many actors and their ability to integrate into the network. That progress will serve as a forcing function to strip away any participants who no longer add value.

Potential Downsides

All technological developments have some negative effects, and blockchain is no exception. With a basic understanding of these technologies and their potential application, a broader set of questions emerges that will keep business, social and government leaders busy for years to come. We'll cover some of these in future publications, but examples include:

- If an individual's data can become a source of income, would the most desirable data come only from society's most well-off citizens? What about those whose data are less valuable due to the individual's lower spending power, or those who have limited access to the digital ecosystem due to economic, physical or other disadvantages? Could blockchain make the "digital divide" worse?
- Will limited access to the connected technologies that enable participation in social, political, personal and work-related functions create a new form of digital poverty?
- How are potentially "absolute" rights of an individual to control how his or her data are used reconciled against the greater good? For example, should an individual be allowed to restrict the use of his or her anonymized health records in new methods of large-scale medical research?

What You Can Do

Every organization benefits from a well-informed workforce, so begin by encouraging your leadership to develop a working knowledge not only of blockchain, but also of the other evolving technologies that are changing the future of work. To identify opportunities and threats on front line, in the back office and everywhere in between, commit to establishing a working literacy at all levels.

References to Mercer shall be construed to include Mercer LLC and/or its associated companies.